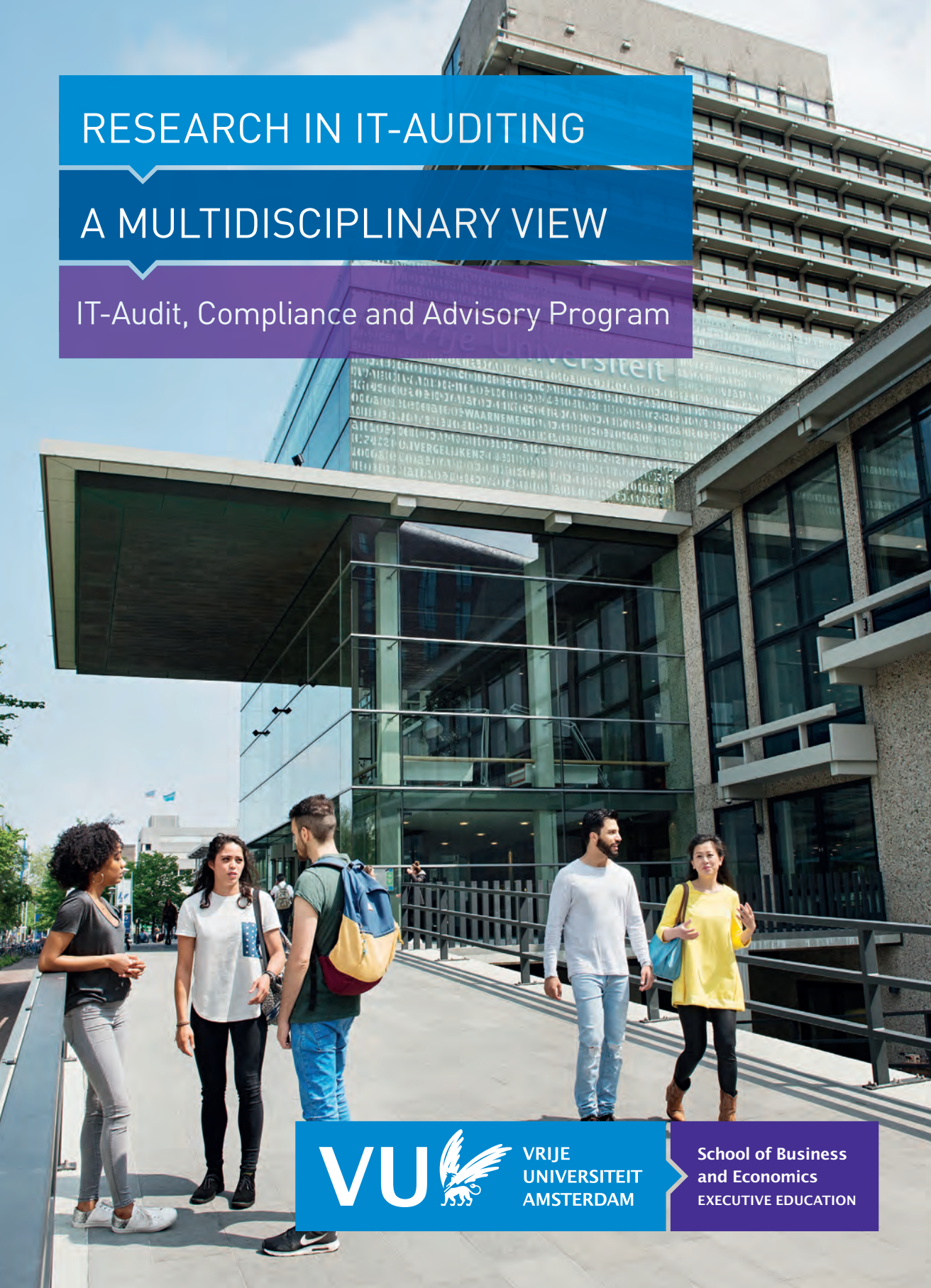
RESEARCH IN IT-AUDITING

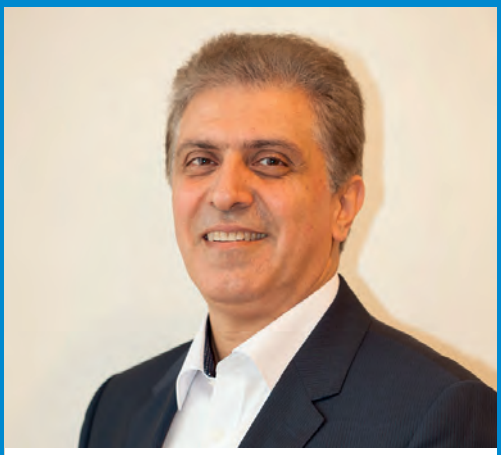
A MULTIDISCIPLINARY VIEW

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
Edition 2019

Omslagontwerp: Jan van Praat/Abbas Shahim
Omslagfoto: 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 978-90-828517-1-7
NUR123

Inhoudsopgave

Preface

Going digital is today's reality and is plainly the only way ahead. Digital technologies[1] have become a mainstream necessity, form the foundation of many organizations, and visibly play their part to steer the success in the current complex and global economy. Those technological advancements have positively impacted diverse sectors, have permeated nearly every single aspect of modern business practices, and have seamlessly turned into a logical starting point. Leaders simply learn to let go on old-fashioned thinking, to take advantage of the arisen unique opportunities, and to benefit from new technologies by transforming towards digital business. In this agile direction, enabling the required change by mainly ensuring a high adoptability level and driving a continuous progress, is clearly a must. It is necessary to keep pace with the speed of market developments, to welcome digital solutions, and to simultaneously handle related issues[2] encountered on the business road in order to become the "new" seriously required these days to grow. Also, digital has left practically no profession unaffected, in particular due to the emergence of powerful technological capabilities possessing the potential that enables to generate value and capture it.
IT-auditing is obviously no exception to the ongoing revolution that explicitly characterizes the digital era. This discipline is currently facing several challenges of different nature too. Among others, it is expected that the IT-auditor performs more with less, designs the work more and more around technology, applies this facility for execution too, decreases the impact of related activities on auditees while delivering the desired quality, and deploys an innovative resourcing model. Hence, traditional structures and classic approaches common in the field will no longer be suitable as a result of which appropriate actions are to be undertaken to overcome the key challenges and demonstrate the ability to satisfy the nowadays expectations. It is evident that embracing the digital mindset as well as transforming the way of auditing will be treated as high strategic priorities for reshaping IT-auditing. These elements are essential to initiate a significant and concerted change that is needed not to lose the momentum of growth and development. This transformational and dynamic journey will accelerate an unforgettable race towards digital value, i.e. the new, that ultimately paves the road for a brighter future for the profession.

Contribution of the book

The articles included in this research-based book are useful for three main reasons. First, these publications shed light on hot topics pertinent to IT-auditing. We are of the opinion that these important subjects are better understood when the underlying philosophies and principles are clarified. Second, the articles share some fresh ideas with respect to revamping the profession and related activities. This way of thinking can make a major contribution to modernize these professional practices. Third, the publications explain the way in which concepts and technologies can pragmatically be utilized. It is our impression that their proper application is valuable to practitioners active in the field. The book thus attempts to reflect described insights, presented views and expounded perspectives in a single bundle that can serve as a helpful source to read and consult in addition to existing materials. Its content can also be used as inspiration for identifying interesting domains for further study. This great deal of documented knowledge, expertise and experience has a story to tell and a lesson to teach. It especially demonstrates our intention to exert positive influence on IT-auditing by contributing to resolving some of its challenges and consequently taking it to the next level.

[1] Examples are Robotic Process Automation (RPA), blockchain and data analytics.

[2] Issues include a higher level of interconnectedness, increasing usage of technological devices, heavily engaging with a larger number of providers, and growing cyber concerns.

Overview of the content

This book contains a collection of comprehensive and well-detailed summaries of various master theses completed at the IT Audit, Compliance & Advisory (ITACA) program. They were written and defended by our graduates who operate in IT-auditing and associated domains. The content of the book is therefore multidisciplinary and explains a wide array of current topics presented in the English as well as in the Dutch language. An overview of the titles incorporated separately in this documented work is shown in the figure below. It is noted here that some of them are abbreviated in order to adequately fit into the illustration.

Suggestions and comments

Your suggestions and comments are valued. We are committed to deliver in accordance with our publishing standards and gladly welcome your feedback. It helps us to maintain a high-quality level and ensures that future books better matches your needs. We look forward to receiving your suggestions and comments that can be provided via email at: edp.sbe@vu.nl. An in-depth session to jointly discuss, share views and define items for the research agenda can obviously be organized as well. We hope that you, as reader, will take the opportunity to read and enjoy this book. In doing so, you will make our efforts worthwhile.

Acknowledgements

I would like to acknowledge and thank Aicha Rahali and the editorial board (Jan van Praat RE RA, Paul Harmzen RE RA, and dr. Rene Matthijsse RE) who made a tremendous effort to create and publish the 2019 version of this book. It is their passion, dedication and teamwork that give life to my idea of an annual academic publication on behalf of the ITACA program. They keep this great tradition alive and demonstrate accordingly our commitment to the IT-audit profession that makes us all proud. I am grateful to the rest of my colleagues for their continuous support: Frank van Praat MSc RE, Stef Schinagl MSc QSA CISA, drs. Kai Hang Ho RE RA, drs. Henk Hendriks RE CISA, drs. Rens Wildenbeest RA, and Paul Visser EMIA CISA. Also, I

thank Ronald Koorn who provided 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

Risk Control Framework related to the Security of Mobile Business Applications

Karima Siamari & Jolien Demoed

	
Jolien Démoed kick-started her IT career by obtaining in 2013 a Bachelor degree in Business Administration and a Master degree in Transport & Supply Chain Management in 2014 at the VU University in Amsterdam. Jolien started working at KPMG IT Advisory in 2015 where she was part of the Risk Consulting team which had a main focus on IT Audit and other assurance related work. During her time at the IT Advisory Risk Consulting department, Jolien graduated from the Executive Master IT Audit, Compliance & Advisory at the VU University in 2018. By 2018, Jolien started to work for the Governance, Risk & Compliance (GRC) department within KPMG. As an IT Auditor and GRC Consultant, Jolien provides ERP and non-ERP related Advisory and Auditing services to national and multinational companies.	Karima Siamari graduated in 2015 with a Bachelor degree in Business Administration and a Master degree in Business Information Management at the Erasmus University Rotterdam. Karima started at KPMG early 2015 as a Research Intern for the purpose of writing her master thesis. After finalising her master thesis, Karima started working at KPMG IT Advisory in 2015 where she was part of the Risk Consulting team with a main focus on IT Audit and Assurance. While working in the IT Advisory Risk Consulting department, Karima graduated from the Executive Master IT Audit, Compliance & Advisory at the VU University in 2018. After working for 2 years in IT Audit and Assurance, Karima switched departments and started to work for the Governance, Risk & Compliance (GRC) department within KPMG IT Advisory. As an IT Auditor and GRC Consultant, Karima focusses on providing Advisory and Audit services in the area of ERP, internal control, and control automation to national and multinational companies.

1 Introduction

Organisations across the globe are developing or making use of mobile applications for their employees to increase productivity. Mobile technology fulfils an increasingly important function within the business. Users have been used to mobile access and apps for some time to retrieve real-time information anywhere at any time. It is therefore no surprise that more organisations are looking for ways to release financial information via mobile devices, for example invoice approval processes where approval can be provided through an application.
Because this is a relative new way of working within organisations this may pose additional challenges (e.g. lost/ stolen mobile devices, mobile application security) with respect to security risks. Also, the already existing challenges (malware, employee security awareness) are not to be neglected. This actualizes the discussion of mobile application security within organisations and the accountability of management for the underlying risks. When identified risks are not addressed well enough through proper risk assessments and implementation of control measures financial data within organisations might become compromised. Literature has identified major risks for mobile devices, however these are not explicitly focused on the technical data security of mobile business applications used in corporate organisations. And in today's world full of IT business transformations, mobile business applications will continue to gather momentum in 2018 despite technical security remaining a concern. Recognizing these risks, organisations will become more responsible for mobile application/ device security. A risk control framework will help the organisations to guide their strategy to control all risks involved and to be able to continuously test and update the security measures. Although a lot of literature and articles is available on technical configurations and settings to protect the mobile environment, related risk control frameworks are not yet in use and do not exist. In literature a gap exists, but this knowledge could be highly useful for IT auditors (internal and external) to control the mobile IT environment.
Numerous large organisations use mobile applications in order to support their operational business processes. This raises the question whether additional measures are needed to cover the related security risks. Based on the outcome of this research, the following research question can be answered:

How should corporate organisations control the risks related to securing mobile business applications?
This thesis focuses on securing mobile business solutions by determining which risks exist and how these could be controlled. The research will be conducted at corporate organisations, which is interesting as these firms provide mobile phones to their employees and are also more likely to encourage their employees to use mobile business applications to achieve maximum efficiency in their work.

2 Theoretical Research

2.1 Mobile business application environment

This section provides a general introduction to the topic under research as well as the scope and outline of the study. Also, it describes the use of mobile business applications at corporate organisations in more detail, specifically focusing on the related risks and controls.

2.1.1 Mobile business applications

Depending on the enterprise, distinct types of mobile devices are in use. These different types of devices should be recorded as a separate mobile device. ISACA categorized mobile devices in three subcategories (ISACA, 2012 ; Cook, 2017):

1 Traditional mobile phones
2 Smartphones, early pocket PC devices.
3 Advanced smartphones, tablet PCs, wearables (such as smart watches).

This thesis focuses on the advanced smartphones (hereinafter referred to as 'mobile devices') that are in use at corporate organisations, which are provided by the organisation to their employees. Being able to trust the device as being a secure platform is critical for allowing mobile access to sensitive organisational data. Nowadays in business, mobile devices have evolved from merely providing access to enterprise e-mail to removing process delays and keeping an eye on the business anytime through the use of mobile business applications. Mobile applications are rapidly becoming the primary communication channel for customers and employees and are therefore expected to be secure and to protect privacy (van Ham, van Iterson & van Galen, 2017).

The use of mobile business applications provides a multitude of advantages and is very useful in daily work life which can be summarized in 3 desired benefits:

- Efficiency – The ability to perform tasks on a mobile app to achieve maximum mobility and benefit from the growing Internet of Things (IoT) capabilities.
- Services provided– The employees should be able to maximize the service they provide customers by being empowered to conduct enterprise-level activities in the same way as on desktop applications .
- Secure – The employees should be able to manage their data securely via the mobile application (van Ham, van Iterson & van Galen, 2017).

2.1.2 Actors involved

Despite numerous benefits described, the use and security of mobile applications in corporate organisations can also pose certain threats. In the context of this thesis, it is necessary to identify the actors involved in relation to mobile business applications to identify potential threats.

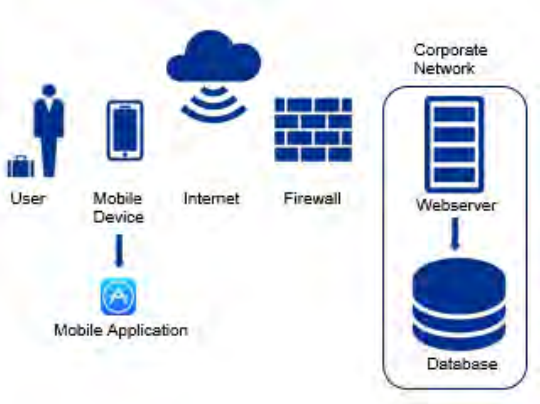


Figure 1: Actors mobile business applications

As shown in figure 1, this includes the following main components (Enisa, 2017):

- User: In this context the user is the employee making use of a corporate mobile device and application.
- Mobile device: this is the mobile device hosting the business applications and OS. In scope of this thesis, the mobile device is provided by the corporate organisation.
- Internet: Internet services accessed from handheld mobile devices.
- Firewall: Firewalls secures web applications by monitoring inbound web traffic for example SQL injections, malware etc. and outbound traffic from the back-end webservers for data loss protection.
- Webserver: Corresponds to the application that hosts the backend of the mobile application (e.g. bank mobile applications connect to the same backend engine of the online bank platform).
- Database: The backend where application data is stored.
- Corporate organisation: As the mobile device provided to employees is managed by the corporate organisation, the corporate network is also an actor involved.

After defining the objects involved in relation to mobile business applications, the possible threats are identified.

2.1.3 Threat analysis

This section contains threats relating to discrete vulnerabilities residing within mobile applications running atop the mobile operating system. The main threats can be summarized in the following (Business of Apps, 2018):

- Sensitive business data could leak via unprotected applications or networks.
- Employees could leave the company and still have access to corporate applications on their mobile devices.
- Mobile devices (which contain sensitive business data) could be lost or stolen.
- Sensitive business data contained in mobile applications is accessed by external parties.
- The employee is responsible for the device, however when there is a lack of mobile security awareness this could lead to security issues when business data (unintentionally) is exposed.

A threat analyses is conducted in order to estimate the impact and likelihood of identified threats. Likelihood is the probability that a threat will manifest itself, the impact is the consequence of the threat manifesting itself associated with costs and quality. Figure 2 presents the results of the threat analysis.

Threats	Impact	Likelihood
Unprotected applications or networks	High	Medium
Leave of employees	Low	Low
Mobile device is lost/ stolen	Low	Low
Access of external parties	High	Medium
Mobile security awareness	High	High

Figure 2: Results threat analysis

Unprotected applications or networks

The impact is high. When network gateways are placed at easily accessible locations and include unpatched vulnerabilities this may enable hackers to control the network gateways and intercept communications (Enisa, 2017). This could lead to severe data protection violations under the recent applicable GDPR legislation. Large organisations are focused towards more structured processes, best security measures and control operations for their Information Technology Management (Chai & Tam, 1997). Consequently, corporate organisations are more likely to have a Mobile Device Management solution in place. Securing applications and networks is still difficult as hackers gain more insights, so the likelihood is medium.

Leave of employees

The impact is defined as low. In case of a malicious employee leaving the company still having access to corporate applications on their mobile device, the impact would be low as this would be an occasional incident and prior authorization restrictions still apply. In addition, corporate organisations are more likely to have an more structured joiner- mover- leaver process in place ensuring the mobile device is handed in in case of a leaver. (Chai & Tam, 1997) For that reason, the likelihood is set on low.

Mobile device is lost/ stolen

Similar to the 'leave of an employee', cases of a lost/ stolen devices are occasional of nature. With the right measures in place, the IT departments can easily wipe the mobile device remotely to make sure business applications (including sensitive data) are secured and cannot be accessed anymore. Therefore the impact and likelihood is low.

Access of external parties
External parties who have access to the network and systems of the organisation are difficult to manage and monitor. External parties are identified as a source of many significant security breaches and are a target for hackers introducing more vulnerabilities and increased risk to the corporate environment. These external parties require high privileged access to networks and therefore impose a high impact if case of misuse.
Corporate organisations provision privileged access by means of a procedure and are more likely to have a structured process in place due to their maturity. Although the amount of vendor accounts is relatively small, it can be challenging to keep track of them, their access rights and monitor their activities on the corporate network. Therefore the likelihood is considered to be medium.

Mobile security awareness
The impact and likelihood on mobile security awareness is high. Employees are considered to be the weakest link in information security (Lineberry, 2007). When there is limited awareness among employees regarding security of mobile devices and the data that is stored in applications/ devices, it could cause a high level of harm to the organisation. In addition employees view security as a hindrance to their productivity (Stone, 2018). The likelihood is therefore considered high.

Considering the above mentioned threats, the growing use of mobile devices within corporate organisations has introduced a higher threat of IT security breaches, misuse of corporate data and reputational damage. The security of mobile devices does not only impacts the business, but also the financial auditor. The auditor verifies the veracity of the financial figures as presented in the annual report. When doing so, the auditor strongly relies on the continuity and reliability of automated data processing, this has been part of the Dutch Civil Code (2:393:4) for many years: "*At least he (the auditor) shall make mention of his findings about the reliability and continuity of computerised data processing.*" The financial auditor relies on the testing of IT Controls performed by the IT Auditor. When a corporate organisation uses mobile business applications as part of their transactional processes, such IT controls could also be implemented in the mobile application itself. As a result, these mobile business application become part of the scope of the financial statement audit.
For the reasons outlined in the theoretical section, it is imperative that mobile business applications are subject to periodic audits performed by IT auditors. In order to effectively perform such an audit it is important to start with a risk assessment and to make use of a control framework designed for mobile business applications.

2.2 Risks related to the security of mobile business applications
All involved actors related to the mobile business applications are identified. However, the aim for this thesis is to focus and narrow down the scope of the actors to only include most relevant actors where corporate organisations are able to influence and mitigate the risks involved. This leads to the following relevant actors:
- User
- Mobile device
- Mobile (business) application
- The link between the mobile device and the corporate network

All other actors are considered to be out of scope. In figure 3, the orange boxed actors are considered to be in scope of this research.

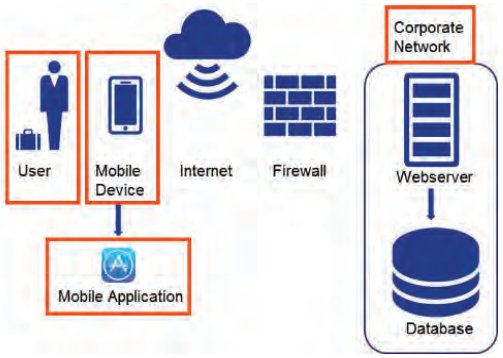


Figure 3: Actors in scope related to mobile business applications

Next to the identification of objects in scope and the threat analysis, risks have been identified per threat area by studying existing literature related to mobile devices/ applications. The identified risks are shown in table 2. During this exercise additional risks were identified outside the defined threat area's which are deemed relevant to the objects in scope and are included as part of the relevant risks (Risk ID 5 and 6).

Threat area	Risk ID	Risk	Risk literature
Leave of employees	11	Mobile devices are not management in a controlled way leading to unauthorised access or unintended leakage of data	ISACA (2012)
Mobile device is lost or stolen	12	Device is lost or stolen and data stored on the device is not backed up	Cooke (2017), ISACA (2012)
	20	Device is lost or stolen leading to data stored on the device being disclosed	ISACA (2012)
Mobile security awareness	17	Employees are not aware of guidelines/ procedures to be followed related to corporate network security.	Symantec (2015), ISACA (2012)
	19	Employees are not using the mobile devices appropriately and securely	Cook (2017), ISACA (2012)
Access of external parties	10	The technical security of the mobile device is insufficient leading to unauthorised access or unintended leakage of data	New gen apps (2017), Khan (2016)
Unprotected applications, devices or networks	01	The technical security setup of the mobile business application is insufficient leading to increased vulnerability or unintended leakage of data	New Gen Apps (2017), Khan (2016)
	02	Authentication to the mobile business application is insufficiently secure	DSWISS (2010)
	03	Improper configuration of session handling leading to malicious session hijacking / unauthorised access	New gen apps (2017)
	04	User authorisations are inaccurate leading to authorisations being too wide and / or Segregation of Duties conflicts	Microsoft.com (2016)
	07	Data is stored in an insecure way making it more easily accessible	New gen apps (2017), Khan (2016), Cook (2017).
	08	Unauthorized access to programs and data on the company network via the mobile business application	Mobile Business Insights (2017), ISACA (2012)

Threat area	Risk ID	Risk	Risk literature
	09	Connections between the mobile devices and corporate network are insufficiently secure leading to unauthorised access and exposure of corporate data	Business of Apps (2018), Cooke (2017)
	10	The technical security of the mobile device is insufficient leading to unauthorised access or unintended leakage of data	New gen apps (2017), Khan (2016)
	13	The cryptography used to ensure corporate data is encrypted, is broken	New gen apps (2017)
	15	Unauthorized access to programs and data on the company network via the mobile business application	Mobile Business Insights (2017), ISACA (2012)
	16	Connections between the mobile devices and corporate network are insufficiently secure leading to unauthorised access and exposure of corporate data	Business of Apps (2018), Cooke (2017), ISACA (2012)
	05	Corporate data is transferred incomplete and/or inaccurate between the mobile business application and the corporate network	(ISACA, 2011)
	06	Data is not processed correctly leading to false output	(ISACA, 2011)

Table 2: Threats per area linked to risks

To conclude, given the research objects in scope, all relevant risks related to mobile business applications are identified which will serve as the basis for identifying related mitigating controls. The research objects, the risks and controls are combined into a Risk Control Framework. The next section describes in more detail the process of establishing the Risk Control Framework which is used in the research related to this thesis.

2.3 Risk Control Framework

This section elaborates on the process of establishing and verifying the completeness of the risk control framework related to the security of mobile business applications (in business context).

2.3.1 Establishing the Risk Control Framework

The theoretical process of analysing theory, identifying relevant object and performing a threat and risk analysis has been depicted in figure 3 and described in previous section. The process of selecting the appropriate controls that relate to the relevant research objects is depicted in figure 4. The control objectives are desired conditions for a research object which, if achieved, minimize the potential that the identified risk will occur. Hence, the control objectives are linked to the identified research objects and are subject to the risks that threaten their chances of achievement. The controls relate to the risks that security of mobile business applications are exposed to and should mitigate the risks.

Figure 3: Theoretical process of defining Risk Control Framework

Figure 4: Establishing the Risk Control Framework

In order to validate the established risk control framework on completeness, the theory of 'Regelkringprincipe' from In 't Veld (1988) and 'Het Vierlagenmodel' (Betz, B., Roelofs, J. & Vrins, J., 1995), is used. Based on performed analyses all identified processes and principles from the theories are covered by one or more controls. In order to further validate the risk control framework on completeness, a mapping is made between a recent issue of the 'IT Security Guidelines for Mobile Apps' by the National Cyber Security Centre (NCSC) published June 2018 (during the thesis research period). All of the defined controls from the NCSC 'IT Security Guidelines for Mobile Apps' are also mapped to one or more controls of the risk control framework. Therefore, the conclusion can be made that the risk control framework is validated on completeness considering the objects in scope of this thesis.

2.3.2 Risk Control Framework (starting point)

Resulting from the theoretical research described in the previous sections, table 3 shows the Risk Control Framework that has been established. This Risk Control Framework is used as a starting point for further research.

Research Object	Control Objective	Risk ID	Risk	Risk Reference	Control ID	Control Description	Control Reference
Mobile Business application	Controls provide reasonable amount of assurance that the mobile application is technical sufficiently secured	1	The technical security setup of the mobile business application is insufficient leading to increased vulnerability or unintended leakage of data	New Gen Apps (2017), Khan (2016)	1.1	A secure (mobile) application lifecycle management policy is in place and includes a specification of the design, development and testing of the application. The security officer is responsible for a yearly sign-off for this policy.	ISACA (2012)
					1.2	A governance is in place for mobile application lifecycle management, specifically, the release of mobile application to the app store and modification of future releases.	ISACA (2012)
					1.3	Binary hardening techniques are standard protocol in application development and enforced at the time of application coding and maintenance.	Khan (2016), ISACA (2016)
					1.4	User/application supplied data is subject to input validation prior to further processing.	New Gen Apps (2017)
					1.5	The mobile business application source code is encrypted according to good-practice market standards to ensure that the code is secret and hard to read.	ISACA (2011)
	Controls provide reasonable amount of assurance that authentication to the mobile business application is sufficiently secure	2	Authentication to the mobile business application is insufficiently secure	DSWISS (2010)	2.1	2/3 factor authentication is enforced when login in to the mobile business application by the user.	DSWISS (2010), ISACA (2012)
					2.2	Login to the mobile business application is limited to the online mode.	New Gen Apps (2017)
	Controls provide reasonable amount of assurance that session handling is appropriately configured	3	Improper configuration of session handling leading to malicious session hijacking / unauthorised access	New Gen Apps (2017)	3.1	When the user has switched from the application, the current session will be terminated. It is not possible to continue with the same session.	New Gen Apps (2017)
					3.2	Users are required to re-authenticate when performing critical actions (such as providing approval on invoices via mobile devices).	New Gen Apps (2017)
	Controls provide reasonable	4	User authorisations are inaccurate leading	Microsoft.com (2016)	4.1	The mobile device access controls are in line with the IT security policy as well as information classification policy.	Cook (2017)

	amount of assurance that authorisations with respect to the mobile business application are sufficiently accurate		to authorisations being too wide and / or SoD conflicts		4.2	Access to the mobile business applications follows the established regular joiner approval process of the company.	ISACA (2012)
					4.3	Authentication to the mobile business application is (automatically) revoked when the employee leaves the company/ access to the corporate network/AD is terminated.	ISACA (2012)
					4.4	Authorisations within the mobile business application are periodically reviewed by the system owner in line with the established authorisation procedures.	ISACA (2012)
					4.5	The review of the authorizations by the system owner is documented and exceptions are followed up accordingly.	ISACA (2012)
	Controls provide reasonable amount of assurance that corporate data is transferred completely and accurately	5	Corporate data is transferred incomplete and/or inaccurate between the mobile business application and the corporate network	International Journal of Education and Information Technologies (2012), ISACA (2011)	5.1	Corporate data is transferred completely and accurately between the mobile business application and the corporate network (by means of checksum, hash total etc.).	ISACA (2011)
	Controls provide reasonable amount of assurance that automated data processing within the mobile business applications works as intended.	6	Data is not processed correctly leading to false output.	ISACA (2011)	6.1	The automated processing in the mobile business application produces the expected results.	ISACA (2012)

Table 3: Risk Control Framework starting point

3 Results

This chapter describes the scope of this research in more detail. Furthermore, section 4.1 provides answer to the third sub question: "To what extent do corporate organisations have controls implemented in practice related to the security of mobile business applications and do these cover the risks involved?". Sections 4.2 and 4.3 provide an answer to the fourth sub question which is defined as follows: "What controls should be implemented to control identified risks related to the security of mobile business applications?"

3.1 Controls implemented in practice versus theory

Through conducting qualitative research by means of interviewing IT experts insight is gained into what extent controls are implemented in corporate organisations in practice. The interview results show that all IT experts were of the opinion that corporate organisation currently do not have official control frameworks established related to mobile business applications. However, all the corporate organisations part of this research do have security measures implemented to control the risks involved that could have an adverse impact on their operational business processes. Due to the recent IT development and IT business transformations they all acknowledge the importance and relevance of performing a risk analysis related to mobile applications/ devices and setting up the associated control frameworks across the whole IT environment (Incl. the mobile IT environment).

This thesis mainly focusses on mobile business applications that could have a financial impact. However, in practice we see that the mobile business applications in use are viewed as potentially highly critical for the supporting and the continuation of the operational business processes. The results also show that a different risk profile exist for the business application depending on the type of organisation and the type of data processed. The importance of a properly executed risk analysis prior to the use is therefore imperative. The control measures that should be implemented is also dependent on the configuration and functionality of the application, the data and risk classification and the type of organisation.

3.2 Outcome discussed per control

This section discusses the results relevant for securing mobile business applications following the conducted interviews with five IT experts. Based on conducted interviews the following logic applies: All the IT experts stress the importance of these controls related to securing mobile business applications in corpo-

rate organisations. Hence, they do acknowledge that these controls should be part of the control framework and remains as initially designed. This accounts for the following controls: 1.1, 1.3, 1.4, 1.5, 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, 4.4, 4.5, 7.2, 10.1, 10.2, 10.3, 10.5, 10.6, 10.7, 11.2, 11.3, 13.1, 13.2, 13.3, 13.4, 17.2, 19.1, 19.2 and 19.3. The remaining controls are discussed below.

Control 1.2 - A governance is in place for mobile application lifecycle management, specifically, the release of mobile application to the app store and modification of future releases.
The IT experts stress the importance of a secure (mobile) application lifecycle management policy and process. However, during the interview we notices some ambiguity in relation to the control description. It was not clear what type of control evidence should be provided and how this control differs from control 1.1. Therefore, it has been decided to change the control description into: *The release of mobile application to the app store and modification of future releases follows the process as described in the mobile application lifecycle management policy.*

Control 4.3 - Authentication to the mobile business application is (automatically) revoked when the employee leaves the company/ access to the corporate network/AD is terminated.
All the IT experts view this control as relevant and important. They stress that it should be clear that revoking the access is part of the regular leaver process of the organisation. To make this clear, the control description has been altered to: *Authentication to the mobile business application is (automatically) revoked when the employee leaves the company and follows the regular leaver process.*

Control 5.1 / 14.1 / 18.1 - Corporate data is transferred completely and accurately between the mobile business application and the corporate network (by means of checksum, hash total etc.).
Four of the five IT experts find this control not relevant in this day and age as the current transmission control protocol and internet protocol (TCP/IP) provide end-to-end data communication specifying how data should be packaged, addressed, transmitted, rooted and received. It has been decided that this control is obsolete and can be removed from the Risk Control Framework.

Control 6.1 - The automated processing in the mobile business application produces the expected results.
The IT experts all find the subject important but would change the control into a monitoring or procedural control. Whether or not this control should be implemented is also dependent on the technical infrastructure underlying the data processing (i.e. in the actual application or direct on the backend). Therefore, it has been decided to change the control description into: *As part of the change management process, specific testing is performed to verify that the mobile business application produces the expected results and is working as designed (i.e. the logic).*

Control 7.1 - Corporate data is not stored on the device itself (the corporate environment is accessible through a virtual session). When the data is stored on the device, it is encrypted.
All the IT experts find this control important. However, during the interview we notices some ambiguity relating to the control description. It was not clear what the control actually intended to achieve. Therefore, to make the purpose of the control clear the control description has been altered to:
When corporate data is stored on the device it is protected in accordance with the information classification policy and the requirements from the IT organisations.

Control 8.1 / 15.1 - Data synchronization of mobile devices is not set to receive access to shared files or network drives that contain data that should be prohibited for mobile use per company policy.
Three of the five IT experts find control relevant but dependent on the information classification. Two of the IT experts do not find this control relevant, in contrary they state that organisations currently want to provide mobile access to the shared files on the internal network drive to their employees. Naturally this has to be done in a safe and secure manner, currently the technical capabilities to do so are available. All the IT experts find the control description not clear. Therefore, the control is altered to: *Mobile access to*

shared files or network drives that contain corporate data is only provided to employees in accordance with the information classification policy and done so in a secure manner following the requirements of the IT organisation.

As this control was a duplicate to control 15.1, it has been decided to remove 8.1 from the research object 'Mobile Device' and remain the control 16.1 at research object 'Corporate Network'.

Control 9.1 / 16.1 - Mobile device users are connecting to the enterprise network via a secure connection, using VPN, IP Security (IPsec), Secure Sockets Layer (SSL) or comparable secure protocols that match good-practice market standards.
All IT experts were of the opinion that having a secure and encrypted connection between the device and corporate network is vital and of utmost importance. To stress the importance of encryption it has been decides to further complete the control description to: *Mobile device users are connecting to the enterprise network via a secure and encrypted connection, using VPN, IP Security (IPsec), Transport Layer Security (TLS) or comparable secure protocols that match good-practice market standards.*
As this control was a duplicate to control 16.1, it has been decided to remove 9.1 from the research object 'Mobile Device' and remain the control 16.1 at research object 'Corporate Network'.

Control 9.2 / 16.2 - Network encryption is implemented to secure all data transferred from a mobile device to the server and back and is aligned with tthe information classification policy.
All the IT experts find this control relevant but the technical implementation of this control is the same as Control 9.1 / 16.1 and up to the organisation to decide how they want to establish a secure and encrypted connection. Therefore, this control is considered to be obsolete and removed from the risk control framework.

Control 9.3 / 16.3 - Data transmitted via WIFI/ 4G connection utilizes at a minimum SSL or TLS protocol for secure transmission of data.
All the IT experts find this control relevant but the technical implementation of this control is the same as Control 9.1 / 16.1 and up to the organisation to decide how they want to establish a secure and encrypted connection. Therefore, this control is considered to be obsolete and removed from the risk control framework.

Control 10.4 / 11.1 - Mobile device management solution is used by the company in order to manage and secure the mobile devices provided to the employees.
All the IT experts find this control most important. As an organisation this is a must to adequately control risks imposed by the use of mobile devices and enforce technical security measures. They have also stressed, that all devices in use should fall under the MDM solution. However, this control is duplicate and included in the same research objects. Control 10.4 is linked to a technical security risk and control 11.1 is related to the risk of managing mobile devices. Therefore, is has been decided to remove control 10.4 and keep control 11.1. Furthermore, to further complete the control description it has been altered to: *Mobile device management solution is used by the company in order to manage and secure the mobile devices provided to the employees. Any attempt to bypass the MDM solution results in immediate disconnection from all corporate resources.*

Control 11.4 - The organisation has established procedures in order to safely destroy discarded mobile devices which may contain corporate data.
All the IT experts view this control as relevant. They suggested to combine control 11.4 and control 11.5 as the related activities are part of the same process. The control description is altered to: *The organisation has established procedures in order to safely destroy, replace or reuse mobile devices which may contain corporate data, ensuring that corporate data is not disclosed.*

Control 11.5 - The organisation has established procedures in order to safely replace or reuse mobile devices, ensuring that corporate data is not being disclosed.
All the IT experts view this control as relevant. This control is combined with control 11.4. and removed from the risk control framework.

Control 12.1 - Data stored on the device is backed up on a separate location accessible to the organisation and/or employee.
All the IT experts were of the opinion that having the data remain accessible is important. However, this control is dependent on the technical setup and infrastructure of the mobile environment. It has been concluded to remain the control as designed.
The control is moved to control objective 7 which is focusing on data storage as well. This order to avoid duplicates. A new control number is established (and control 12.1 is removed from the framework):

Control 7.3 (NEW): *Data stored on the device is backed up on a separate location accessible to the organisation and/or employee.*

Control 17.1 - An IT security policy exist and includes guidelines and procedures with regards to securing the corporate network which is enforced by management.
All the IT experts agreed with the control description. Having an overall IT Security policy in place is a must for all corporate organisations. However, in order to emphasize the mobile aspect, the conclusion has been made to alter the control description to: *An IT security policy exist and includes guidelines and procedures with regards to securing the corporate network related to connecting to mobile devices which is enforced by management.*

Control 19.4 - Employees are trained on a regular basis to be aware of the potential damage of malicious application downloads (applications not issued by the company).
All IT experts view this control as important and providing trainings to employees is very important to make sure they know how to recognize and respond to the different mobile security risks. However, one of the IT experts stressed that training provided should be broader and focus on all mobile security risks and not only malicious applications. For example, subjects as losing your phone, not installing application outside the regular app store, no jail breaking / rooting your phone etc. Therefore, it is concluded to alter the control description to: *Employees are trained on a regular basis to be aware of all the potential mobile security risks, to enable them to recognize and properly respond to these risks in accordance with the IT security policy.*

Control 20.1 - A protocol exist to report and handle lost or stolen mobile devices which is known to all employees.
All IT experts find this control relevant and important that the employees are aware what to do when their device is stolen or lost and how to report this. In order to further clarify the control description it has been altered to: *All employees know how to report on lost or stolen devices by means of a process description which is accessible to everyone in the organisation (e.g. via intranet).*

Control 20.2 - Mobile device (security) incidents management processes are established in the organisation and monitored on a regular basis.
All IT experts view this control as important and stress that mobile security incidents are part of the regular incident management process. The control description is changed to: *Mobile device (security) incidents are handled through the established regular incident management processes in the organisation and monitored on a regular basis.*

Control 20.3 - An asset management procedure is in place for tracking mobile devices, including procedures for lost and stolen devices as well as employees who have been terminated or have resigned from the enterprise.

All IT experts view this control as relevant and having asset management in place should be standard for corporate organisations. Two of the five IT experts suggested to change the formulation of the control. Tracking triggers the wrong impression as it suggest following individuals. Therefore, it has been decided to alter the control description to: *An asset management procedure is in place for registering mobile devices which includes the attributes (e.g. basic software aspects, installed business applications, corporate data access and classification) that should be captured which is in line with the information classification policy.*

Control 20.4 - A CMDB is used within the organisation for tracking mobile devices. This is linked to the information classification policy, and is updated periodically. A CMDB owner has been appointed.
All IT experts view this control as relevant as a CMDB is used to keep track of mobile devices in use. Making use of a CMDB is part of the asset management procedure, therefore is makes more sense to link this control to the asset management procedure. The control description is changed as follows: *A CMDB is used within the organisation for registering mobile devices and is updated periodically. This CMDB is part of the asset management procedure and a CMDB owner has been appointed to manage all assets.*

Control 20.5 - The company is able to remotely wipe data stored on lost or stolen devices by making use of mobile device management solution.
All the IT experts view this control as relevant and as something they would implement. However, the relevance of this control does depend whether or not corporate data is stored on the device. One IT expert states that wiping alone is not sufficient, the importance of encryption of the device and application is also stressed. Also, enabling corporate organisations to wipe mobile devices is managed through MDM. Therefore, it is decided to alter the control description and include this in control objective 11 (managing mobile devices). The new control is as follows:

Control 11.6 (NEW) *- Mobile device management solution is used to enable the organisation to remotely wipe data stored on lost or stolen devices.*

3.3 Risk Control Framework (scoped and final)

Based on the results found by conducting this research the initial Risk Control Framework was validated in practice and finalised to deliver the controls that should be implemented by corporate organisations in order to mitigate the identified risks related to the security of mobile business applications. Table 4 shows the final Risk Control Framework, as the deliverable of this thesis research.

Research Object	Control Objective	Risk ID	Risk	Control ID	Control Description
Mobile Business application	Controls provide reasonable amount of assurance that the mobile application is technical sufficiently secured	1	The technical security setup of the mobile business application is insufficient leading to increased vulnerability or unintended leakage of data	1.1	A secure (mobile) application lifecycle management policy is in place and includes a specification of the design, development and testing of the application. The security officer is responsible for a yearly sign-off for this policy.
				1.2	The release of mobile application to the app store and modification of future releases follows the process as described in the mobile application lifecycle management policy.
				1.3	Binary hardening techniques are standard protocol in application development and enforced at the time of application coding and maintenance.
				1.4	User/application supplied data is subject to input validation prior to further processing.
				1.5	The mobile business application source code is encrypted according to good-practice market standards to ensure that the code is secret and hard to read.
				1.6	Common leakage points/ vulnerabilities are monitored by the IT organization on a regular basis by means of specialized tooling and resolved accordingly.
	Controls provide reasonable amount of assurance that authentication to the mobile business application is sufficiently secure	2	Authentication to the mobile business application is insufficiently secure	2.1	2/3 factor authentication is enforced when login in to the mobile business application by the user.
				2.2	Login to the mobile business application is limited to the online mode.
	Controls provide reasonable	3		3.1	When the user has switched from the application, the current session will be terminated. It is not possible to continue with the same session.

Research Object	Control Objective	Risk ID	Risk	Control ID	Control Description
	amount of assurance that session handling is appropriately configured		Improper configuration of session handling leading to malicious session hijacking/ unauthorised access	3.2	Users are required to re-authenticate when performing critical actions (such as providing approval on invoices via mobile devices).
	Controls provide reasonable amount of assurance that authorisations with respect to the mobile business application are sufficiently accurate	4	User authorisations are inaccurate leading to authorisations being too wide and / or SoD conflicts	4.1	The mobile device access controls are in line with the generic IT security policy and information classification policy.
				4.2	Access to the mobile business applications follows the established regular joiner approval process of the organization.
				4.2	Access to the mobile business applications follows the established regular joiner approval process of the company.
				4.3	Authentication to the mobile business application is (automatically) revoked when the employee leaves the company and follows the regular leaver process.
	Control provide reasonable assurance that automated data processing within the mobile business applications works as intended.	6	Data is not processed correctly leading to false output	6.1	As part of the change management processes, specific testing is performed to verify that the mobile business application produces the expected results and is working as designed (i.e. the logic).
Mobile device	Controls provide reasonable amount of assurance that corporate data is stored appropriately secured	7	Data is stored in an insecure way making it more easily accessible	7.1	When corporate data is stored on the device it is protected in accordance with the information classification policy and the requirements from the IT organisations.
				7.2	Mobile device encryption settings are in line with the IT security as well as information classification policy of the company.
				7.3	Data stored on the device is backed up on a separate location accessible to the organisation and/or employee.
	Controls provide reasonable amount of assurance that the mobile device is sufficiently secured	10	The technical security of the mobile devices insufficient leading to unauthorised access or unintended leakage of data	10.1	Mobile device antivirus software is updated regularly to prevent perpetuation of malware.
				10.2	Patch and Vulnerability processes are established in the organisation. Mobile devices are subject to these processes and regularly updated.
				10.3	Common leakage points/vulnerabilities are monitored by the IT organization on a regular basis by means of specialized tooling, and resolved accordingly.
				10.6	The corporate and private environment are separated on the mobile device (Chinese wall).
				10.8	Mobile device management technically enforces that unsigned third party apps, which may carry malware or provide a gateway for malicious outsiders to enter the corporate network, cannot be installed on the mobile device.
				10.9	Mobile device management technically enforces that sharing possibilities of data between the mobile business application and third party applications is restricted according to the information classification policy.
	Controls provide reasonable amount of assurance that mobile devices are managed in a controlled way	11	Mobile devices are not management in a controlled way leading to unauthorised access or unintended leakage of data	11.1	Mobile device management solution is used by the company in order to manage and secure the mobile devices provided to the employees. Any attempt to bypass the MDM solution results in immediate disconnection from all corporate resources.
				11.2	`Mobile devices are required to register for the mobile device management solution of the company when provisioned to employees.
				11.3	The technical security measures enforced by the mobile device management solution are periodically reviewed and updated by the security officer / security responsible.
				11.4	The organisation has established procedures in order to safely destroy, replace or reuse mobile devices which may contain corporate data, ensuring that corporate data is not disclosed.
				11.6	Mobile device management solution is used to enable the organisation to remotely wipe data stored on lost or stolen devices.
	Controls provide reasonable amount of assurance that corporate data is securely encrypted	13	The cryptography used to ensure corporate data is encrypted, is broken	13.1	Secure key management procedures are established and documented, including key generation, key distribution, key storage and key destruction. The role of key custodians, operators, key owners and KMS users are also defined in the policy.
				13.2	Key management procedures are periodically tested / dry run by the IT organisation, to ensure that the procedures work effectively.
				13.3	Cryptography keys are stored in not easily accessible locations or are hard coded.
				13.4	The use of superior encryption protocols (i.e. not generally known to be broken) is standard protocol in mobile business application life cycle.
Corporate Network	Controls provide reasonable amount of assurance that the connection between the mobile device and corporate network is appropriately secured	16	Connections between the mobile devices and corporate network are insufficiently secure leading to unauthorised access and exposure of corporate data	15.1	Mobile access to shared files or network drives that contain corporate data is only provided to employees in accordance with the information classification policy and done so in a secure manner following the requirements of the IT organisation.
				16.1	Mobile device users are connecting to the enterprise network via a secure and encrypted connection, using VPN, IP Security (IPsec), Transport Layer Security (TLS) or comparable secure protocols that match good-practice market standards.
	Controls provide reasonable amount of assurance that mobile devices are appropriately used by employees.	17	Employees are not aware of guidelines/ procedures to be followed related to corporate network security.	17.1	An IT Security policy exist and includes guidelines and procedures with regards to securing the corporate network related to connection to mobile devices which is enforced by management.
				17.2	The IT security policy is periodically reviewed by the IT organization/ security officer and updated accordingly.

Research Object	Control Objective	Risk ID	Risk	Control ID	Control Description
User	Controls provide reasonable amount of assurance that mobile devices are appropriately used by employees	19	Employees are not using the mobile devices appropriately and securely	19.1	An Acceptable Usage policy for mobile devices exist and includes rules for appropriate physical and logical handling, addresses mobile device use and specifies the type of information and services that may be accessible through the devices.
				19.2	Employees are required to sign a statement that they have read, understood and will comply with the Acceptable Usage policy for mobile devices including the rules for appropriate physical and logical handling.
				19.3	An awareness program is in place that addresses the importance of securing the mobile devices physically and logically. The training includes the types of information that can and cannot be stored on mobile devices.
				19.4	Employees are trained on a regular basis to be aware of the potential mobile security risks to enable them to recognize and properly respond to these risks in accordance with the IT security policy.
	Controls provide reasonable amount of assurance that mobile devices and security incidents are appropriately managed by employees	20	Device is lost or stolen leading to data stored on the device being disclosed	20.1	All employees know how to report on lost or stolen devices by means of a process description which is accessible to everyone in the organisation (e.g. via intranet).
				20.2	Mobile device (security) incidents are handled through the established regular incident management processes in the organisation and monitored on a regular basis.
				20.3	An asset management procedure is in place for registering mobile devices including the attributes that should be captured (e.g. basic software aspects, installed business applications, corporate data access) and is in line with the information classification policy.
				20.4	A CMDB is used within the organisation for registering mobile devices and is updated periodically. This CMDB is part of the asset management procedure and a CMDB owner has been appointed manage all assets.

Table 4: Risk Control Framework (scoped and finalised based on results)

4 Conclusion

This thesis researched the security of mobile business application from an IT audit perspective. The focus was to provide a risk control framework that can be used in practice. Literature on existing risk control frameworks was studied and articles on the mobile technical security were read in order to form a basis for this research. By using the qualitative research method, the opinions of IT experts were combined with the studied literature.

4.1 Conclusion: answer to the main Research Question

The research question as proposed in the introduction is:

'*How should corporate organisations control the risks related to securing mobile business applications?*'

The research question was answered by using the qualitative research method. It can be concluded that the established and validated risk control framework can be used by the corporate organisations in order to continuously test and update technical measures related to usage of mobile business applications in order to safeguard the organisation and it's highly sensitive data.

Controls related to the technical setup of the mobile business application and a secure application life cycle management are vital and need to be taken into account. These controls are focussing on tracking the risk of an application as it moves through the development lifecycle. Binary hardening, input validation and encryption complement a secure development environment to prevent vulnerabilities and unintended leakage of data from unprotected applications. These controls are even more relevant for mobile business applications as they might contain high sensitive corporate data and the fact that mobile devices are often used outside the corporate organisation.

Securing the mobile business application by means of sufficient authentication and authorisation configuration is relevant for the mobile business applications, but this highly dependent on how the IT infrastructure and the mobile environment has been set up. As this research has shown, even though it could be that part of the authentication logic is performed by the back end server, it is important to consider this as integral part of the mobile architecture.

A major difference between the mobile device and a desktop is that mobile devices are able to stay continuously connected to the web and they are designed to be taken everywhere with you. However, this poses also a lot of risks. Therefore the controls related to secure data storage as part of research object Mobile Device can be found in the finalized risk control framework.

In order to prevent unauthorised access and unintended leakage of corporate data it is also vital to incorporate the right technical security measures to protect the mobile device (e.g. anti-virus, patch and vulnerabilities, separate corporate and private environment and data sharing).
In order to steer the corporate organisations in their strategy to control their mobile environment, also controls related to Mobile Device Management solutions are incorporated. As this research shows, a Mobile device management solution will provide IT controls needed to secure, manage and monitor corporate owned devices that access sensitive corporate data.
In addition, this research shows that cryptography on mobile device controls are inevitable. As the mobile devices might consist of high sensitive corporate data it demands a secure manner of protecting the data using cryptographic techniques. Controls related to cryptography will add value to the corporate organisations strategy in protecting their data stored on mobile devices.
Second last, this research implied also to include controls related to securing the corporate network. As indicated earlier, mobile devices should be highly protected from external threats. Therefore when connecting to the corporate network, high security standards should be incorporated to protect the corporate organisation from exposure of corporate data. Controls related to these security standards will guide the organisation how to continuously monitor and test to ensue secure connection between mobile device and corporate network.
At last, a well-known sentence in the world of security is that the 'people are the weakest link in cyber security risks'. The established risk control framework could not be finalized without incorporating 'soft controls' related to the user of the mobile device.
In conclusion, there are number of significant controls a corporate organisation should have in place in order to securely make use of mobile business applications. To summarize this means controls related to: secure development, technical setup, authentication & authorizations, cryptography, sessions handling, using MDM, connections with corporate network and the user.
However, it must be said that how corporate organisation control their mobile environment is also dependent on a few factors. It is of upmost importance to perform risk assessments to identify the IT maturity of the organisation, risk appetite and how the mobile infrastructure has been set up. The established framework can be adjusted to this analysis, by verifying the controls that are applicable to the organization.

5 Limitations and Future Research

As with any research conducted, the research done to write this thesis is also subject to a number of limitations which should be taken into accounts when interpreting the results obtained.
To start off, due to time- and budget restrictions this research was not conducted on a large scale. A total of five IT experts from several corporate organisation were included in the research. Another limitation is the limited sample size compared to the population. In order to be able to meaningfully generalise the conclusions of this research to the entire population, the sample size should have been much larger. However, the previous limitation prevented the researchers to do so. Another limitation lies in the interview methodology used in this study. This results in that certain concepts can mean different things to different people, dependent on their prior experiences and their interpretation of the questions. Furthermore, human interaction naturally introduces a bias to provide socially desirable answers. Compared to other research methods, interviews are more subject to bias and interpretation. Only corporate organisations have been included in this research which are in many aspects very different from small and mid-size companies. Generalising these results towards all organisations might not be practical. Also, the corporate organisations which were researched were all trade and/or service companies. Corporate organisations highly dependent on IP/ business critical data for their going concern might have a different risk appetite towards securing their IT environment including the use of mobile business applications. This might impact meaningfully generalising the conclusions to all corporate organisations. The aforementioned combined, the conclusions of this study should be interpreted taking these limitations into account.

As mobile business applications becomes increasingly more important there is an apparent opportunity for further research into gaining a more extensive understanding. A market development can be observed where mobile devices on the go are converging more and more, the differences between mobile phones, tablets and laptops and similar devices are diminishing. This research has focussed specifically on mobile devices (i.e. mobile phones) providing an opportunity to research security risks taking this trend and the area of end-device security into account. Different organisation types might have different risk appetites, adoption of mobile devices, level of technology enablement etc. Market/ industry specific research might render more specific results when adjusting for context specific factors, for example intellectual property. Technology develops in a fast pace, this research might be outdated in a couple of years/ near future. According to the NCSC corporate organisations are also increasingly using mobile business applications. This might lead to an increased pace of development, different views etc. Re-conducting this research and/or on a larger scale in a couple of years will thus likely result in new insights. Other research methods could also be utilized which might lead to different results.

6 References

6.1 Articles

Bernik, I. & Markelj, B. (2012). Mobile Devices and Corporate Data Security. *International Journal Education and Information Technologies, 1(*6).

Betz, B., Roelofs, J. & Vrins, J. (1995). Integraal ontwikkelen van organisatie en informatiesystemen, *Kluwer Bedrijfsinformatie.*

Chau, P.Y., & Tam, K.Y. (1997). Factors affecting the adoption of open systems: an exploratory study. *MIS quarterly, 1*(24).

Lineberry, S. (2007). The Human Element: The Weakest Link in Information Security. *Journal of Accountancy; New York, 24*(5), 44-46,49.

van Ham, D., van Iterson, P. & van Galen, R. 2017. Mobile Landscape Security, Addressing security and privacy challenges in your mobile landscape, *KPMG*.

ISACA, 2011. *CISA Review Manual 2011.*

ISACA, 2010. *Securing Mobile Devices.*

In 't Veld, J. (1988), Analyse van organisatieproblemen. Een toepassing van denken in systemen en processen, *Stenfert Kroese*.

National Cyber Security Center (NCSC – NL), 2018. *IT Security Guidelines for Mobile Apps.* Den Haag.

6.2 Websites

Cooke, I. (2017). IS Audit Basics: Auditing Mobile Devices. *ISACA Journal,* (6). Retrieved June 15, 2018, from https://www.isaca.org/Journal/archives/2017/Volume-6/Pages/auditing-mobile-devices.aspx

SAP. Time and attendance in the cloud to improve workforce performance. Retrieved June 15, 2018, from: https://www.sap.com/products/human-resources-hcm/labor-time-attendance-management.html

Enisa (2017). Privacy and data protection in mobile applications. Retrieved June 22, 2018, from: WP2017 O-2-2-4 GDPR Mobile.pdf

DWISS(2010). 2-Factor authentication for mobile applications: Introducing Doublesec. Retrieved June 22, 2018, from: https://digitalcollection.zhaw.ch/bitstream/11475/1827/1/2010_Renn_2-FACTOR_ZHAW.pdf

Business of Apps (2018). How to Secure Your Enterprise Mobile Applications. Retrieved June 23, 2018, from: http://www.businessofapps.com/how-to-secure-your-enterprise-mobile-applications-2/

Microsoft, 2016. Authentication and authorization in Azure App Service for mobile apps. Retrieved July 6, 2018, from: https://docs.microsoft.com/en-us/azure/app-service-mobile/app-service-mobile-auth

Mobile Business Insights (2017). Offline data synchronization, Part 1: Basic strategies to address this critical challenge for mobile apps. Retrieved August 10, 2018, from: https://mobilebusinessinsights.com/2017/09/offline-data-synchronization-part-1-basic-strategies-to-address-this-critical-challenge-for-mobile-apps/

New gen apps (2017). 10 Biggest Risks to Mobile Apps Security. Retrieved August 3, 2018, from: https://www.newgenapps.com/blog/10-biggest-risks-to-mobile-apps-security

Stone, M. 2018. How Effective Is Security Awareness Training for Threat Prevention? *Security Intelligence*. Retrieved July 6, 2018, from: https://securityintelligence.com/how-effective-is-security-awareness-training-for-threat-prevention/

Symantec (2015). Training Your Employees on Information Security Awareness. Retrieved August 10, 2018, from: https://www.symantec.com/connect/blogs/training-your-employees-information-security-awareness

TechOpedia (n.d.). Technical Security. Retrieved September 7, 2018, from: https://www.techopedia.com/definition/31429/technical-security-techsec

Zekerheid omtrent een stabiele productieomgeving bij het gebruik van DevOps

Jurgen Diters

Jurgen Diters graduated for the Master Information and Knowledge Management by 2014 at the Vrije Universiteit (VU) in Amsterdam. He joined the Ernst & Young IT Risk & Assurance (ITRA) practice in Amsterdam, focussing on financial audit and IT integration.

Jurgen works as an IT auditor, performing IT audits at large national and international organizations and has experience in auditing various ERP systems. Since 2018 he is part of the “Cyber in the Audit” team within EY, working on integrating cyber topics in the current IT audit framework. Jurgen also has several years of experience in performing Quality Assurance (Q&A), data analystics and service organization control reporting.

1 Inleiding

Volgens Gartner (2016) zijn wereldwijde IT-organisaties bezig met een constante zoektocht om de meest recente softwareproducten te produceren om aan de vraag van de klant te voldoen. DevOps wordt steeds meer het antwoord voor het bereiken van het doel van voortdurende product uitrollen die ontworpen zijn om concurrenten te overtreffen met ongeëvenaarde aanbiedingen. Gartner definieert DevOps als een verandering in de cultuur, gericht op een snelle levering van IT-services door het gebruik van agile en lean methoden. DevOps legt de nadruk op mensen (en cultuur) en streeft ernaar de samenwerking tussen beheerteams en ontwikkelteams te verbeteren. DevOps implementaties maken gebruik van slimme technologie, waaronder automatiseringstools. Deze benutten een steeds meer programmeerbare en dynamische infrastructuur.

DevOps gaat voornamelijk om het verkorten van de cyclustijd die vereist is voor het vrijgeven van applicaties. Agile werken zorgde voor een verschuiving van ontwikkelingscycli van enkele maanden naar kortere 'sprints' van meestal een paar weken. Onder DevOps kan elke cyclus uren of minuten in plaats van weken zijn. John Jenkins, de voormalig hoofdingenieur van Amazon, zei bijvoorbeeld dat Amazon tijdens een werkweek elke 12 seconden nieuwe code naar productie pusht. Historisch (d.w.z. voorafgaand aan DevOps) zou een cyclustijd gemeten in seconden of minuten ongehoord zijn; nu is dit tempo echter niet alleen haalbaar, maar in veel gevallen ook de gewenste staat (Moyle, 2015).

Zeer complexe en bedrijfskritieke software wordt vaak door gedistribueerde teams ontwikkeld. Een nauwere connectie tussen de ontwikkeling en de uitvoering is vereist om ervoor te zorgen dat fouten zo snel mogelijk worden gedetecteerd en opgelost (Fitzgerald & Stol, 2017). Volgens Rahman et al. (2016) richt DevOps zich op samenwerking tussen verschillende teams in een organisatie om een snelle implementatie van software en services voor eindgebruikers te bereiken, mede door de software-afleveringsinfrastructuur te automatiseren. Vooral de samenwerking tussen het ontwikkelaars en het beheerteam is cruciaal in het laten slagen van DevOps (Humble & Farley, 2010). Het doorvoeren hiervan vergt een hoge mate van automatisering zodat handelingen binnen het proces snel en foutloos kunnen worden uitgevoerd.

DevOps is een organisatorische aanpak om barrières tussen teams in een organisatie te verminderen en daarmee de ontwikkeling en implementatie te versnellen. Steeds meer organisaties voor softwareontwikkeling erkennen het belang van snelle, betrouwbare en voorspelbare software van hoge kwaliteit. Toch worstelen ze er vaak mee om de juiste benaderingen en werkwijzen met betrekking tot het softwareleveringsproces te implementeren (Dyck et al., 2015).

Volgens de resultaten van een van de studies van CA Technologies (2014) over de applicatie-economie en de rol van DevOps, heeft 88% van de 1.425 managers binnen de komende vijf jaar DevOps geadopteerd. Een soortgelijke wereldwijde studie van CA Technologies uit 2013 laat eveneens zien dat 66% van de 1300 senior IT managers reeds gebruik maakte van DevOps of van plan waren op korte termijn te adopteren. De stijging in het percentage van managers dat gebruik maakt van DevOps kan verklaard worden door een grotere vraag van IT om productiecode te leveren en daarnaast de zichtbare voordelen die men ervaart bij het gebruik van DevOps. Volgens CA Technologies (2014) zijn de tastbare voordelen die organisaties ervaren met DevOps verbeterd met 15% tot 21%.

Organisaties die gebruik maken van DevOps ervaren 60 keer minder fouten en herstellen 168 keer sneller dan organisaties die geen gebruik maken van DevOps. Daarnaast brengen ze 30 keer meer wijzigingen naar productie met 200 keer kortere doorlooptijden (Puppet Labs, 2016). Ondanks de populariteit die de DevOps heeft weten te winnen, blijven de beveiligingsaspecten omtrent DevOps een zorg voor organisaties die DevOps willen adopteren (CA Technologies, 2014). Ontwikkelaars die DevOps gebruiken kunnen hun softwarewijzigingen in hoog tempo vastleggen en implementeren met behulp van een geautomatiseerd proces. In een dergelijk hoog tempo, wanneer het beveiligingsteam afzonderlijk opereert zonder nauwe samenwerking met het ontwikkelteam en beheerteam, zullen de softwarewijzigingen mogelijk niet de juiste beveiligingsmaatregelen ondergaan en leiden tot kwetsbare software. Door beveiligingsmaatregelen

in het DevOps proces te integreren, in de fasen van ontwikkeling, testen en implementatie, kunnen organisaties de kwaliteit van de software verbeteren (Rahman, Ashfaque & Williams, 2016).
Volgens Rahman, Ashfaque & Williams (2016) draagt het automatiseren van monitor activiteiten, automatiseren van test activiteiten en het automatiseren van code reviews bij aan het integreren van de beveiliging in DevOps. Daarnaast stellen ze dat beveiligingsteams nauw dienen samen te werken met het multidisciplinaire DevOps team. Onderdeel hiervan zijn ook testers, omdat testen een sleutelelement is om foutloze releases te garanderen (Humble & Farley, 2010).

2 Onderzoeksvragen

De betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking bij het gebruik van de waterval methode is al uitgebreid bestudeerd door verschillende auteurs. Het waarborgen van een stabiele productieomgeving bij het gebruik van de DevOps methode is een onderwerp dat nog moet worden onderzocht. Hierbij dient men wel onderscheid te maken inde aard van de gegevensverweking. De volgende onderzoeksvraag staat centraal in deze scriptie:
'Welke maatregelen moeten genomen worden om een stabiele productieomgeving te realiseren bij het gebruik van DevOps?'
De onderzoeksvraag zal worden beantwoord door middel van de volgende deelvragen:
- Wat is DevOps?
- Wat is een stabiele productieomgeving?
- Welke beheersingsmaatregelen zijn relevant gericht op een stabiele productieomgeving?
- Welke additionele risico's gaan gepaard met de adoptie van DevOps en door middel van welke beheersingsmaatregelen kunnen deze risico's gemitigeerd worden?

Deze scriptie zal bijdragen aan onderzoek omdat het beter inzicht geeft in de factoren die van invloed zijn op het behouden van een stabiele omgeving. Deze scriptie is een van de eerste pogingen om de waargenomen verschuivingen van de risico's binnen de agile-beheersprocessen te onderzoeken. Deze scriptie kan vervolgens worden gebruikt als een startpunt voor toekomstig onderzoek naar de DevOps binnen additionele kaders. In de praktijk zullen organisaties beter kunnen begrijpen welke beheersingsmaatregelen zij zullen moeten inrichten om zo een stabiele productieomgeving te behouden bij het gebruik van DevOps. Daarnaast zullen de uitkomsten van deze scriptie gebruikt kunnen worden door auditors die hiermee voor DevOps specifieke beheersingsmaatregelen kunnen opnemen in het door hen te testen raamwerk.

3 Literatuuronderzoek

In dit hoofdstuk wordt er nader ingegaan op het begrip DevOps en zal er een definitie gekozen worden die als uitgangspunt wordt gehanteerd in deze scriptie. Vervolgens worden de manieren om agile software te ontwikkelen besproken en wordt nader ingegaan op de stabiele productieomgeving. Als laatst wordt uiteengezet wat er in de literatuur reeds bekent is over het automatiseren van beheersmaatregelen.

3.1 DevOps

DevOps kent tot op heden nog geen uniforme definitie. Als gevolg hiervan gebruiken veel mensen eigen definities of vertrouwen ze op derden, wat resulteert in verwarring over het begrip DevOps.
Volgens Dyck et al. (2015) zijn er twee populaire DevOps definities gegeven door Hüttermann (2012) en Gene Kim (2014). Hüttermann definieert DevOps als "a mix of patterns intended to improve collaboration between development and operations. DevOps addresses shared goals and incentives as well as shared processes and tools".
Kim geeft een andere definitie van DevOps, namelijk "The term 'DevOps' typically refers to the emerging professional movement that advocates a collaborative working relationship between Development and IT

Operations, resulting in the fast flow of planned work (i.e., high deploy rates), while simultaneously increasing the reliability, stability, resilience and security of the production environment".
In het boek van Bass, Weber & Zhu (2015) wordt DevOps als volgt gedefinieerd:
"DevOps is a set of practices intended to reduce the time between committing a change to a system and the change being placed into normal production, while ensuring high quality".
Daarbij worden in het boek vijf verschillende toepassingen beschreven die deze definitie onderschrijven:

- De beheerafdeling verantwoordelijk maken voor de vereisten van wijzigingen. Dit is in overeenstemming met het aspect 'high quality' zoals in de definitie.
- Het ontwikkelteam verantwoordelijk maken voor de incident afhandeling. Dit zorgt ervoor dat de tijd tussen het ontdekken van een fout en het herstel van die fout wordt verkleind.
- Afdwingen dat het implementatieproces door iedereen wordt gebruikt, inclusief ontwikkelaars en het beheerteam. Hierdoor wordt de kwaliteit van de implementaties vergroot en worden fouten vermeden die worden veroorzaakt door ad-hoc implementaties.
- Gebruik maken van 'continuous deployment'. Dit zorgt voor een kortere doorlooptijd tussen het ontwikkelen van de wijziging en de uiteindelijke in productiename.
- Infrastructuurcode, zoals implementatiescripts, zullen met gelijke vereisten als applicatiecode moeten worden ontwikkeld. Dit zorgt ervoor dat de kwaliteit van de applicatie wordt gewaarborgd en dat implementaties verlopen zoals gepland.

Bovenstaande definities beperken zich tot de samenwerking tussen 'development' en 'operations'. DevOps integreert namelijk de twee werelden van ontwikkeling en operations, met behulp van geautomatiseerde ontwikkeling, implementatie en monitoring van de IT infrastructuur. Het is een organisatorische verschuiving waarin, in plaats van gedistribueerde groepen die taken afzonderlijk van elkaar uitvoeren, cross-functionele teams werken aan continue levering van nieuwe software functionaliteit. DevOps helpt in het sneller en beter leveren van toegevoegde waarde, waardoor problemen afnemen als gevolg van betere communicatie tussen teamleden en het oplossen van problemen wordt versneld (Ebert et al., 2016). Turk et al. (2014) maken hierbij wel de kanttekening dat bedrijven die gebruik maken van grote complexe legacy systemen, mogelijk geen agile processen in hun huidige vorm kunnen gebruiken.
Hoewel DevOps een afkorting is van 'development' en 'IT operations' is het volgens Dyck et al. (2015) niet beperkt tot die twee teams. Over het algemeen lijkt er overeenstemming te zijn dat DevOps gaat over het verbeteren van de communicatie en samenwerking tussen teams in een organisatie of project. Zowel ontwikkelingsdoelen als beheerdoelen zijn even belangrijk, aangezien ontwikkelsystemen en onderhoudssystemen gezamenlijk door beide partijen moeten worden bediend. De organisatie van DevOps team valt derhalve tevens onder de verantwoordelijkheid van zowel de business als IT. Daarnaast stellen Dyck et al. (2015) dat de focus moet liggen op 'resilient systems, ofwel software en de productie omgeving. Hieruit volgt de volgende definitie:
"DevOps is an organizational approach that stresses empathy and cross-functional collaboration within and between teams – especially development and IT operations – in software development organizations, in order to operate resilient systems and accelerate delivery of changes".
Voor dit onderzoek wordt de laatst genoemde definitie als uitgangpunt gehanteerd.

3.1.1 Continuous Integration

Continuous Integration (CI) is een van de manieren om agile software te ontwikkelen, waarbij elk teamlid steeds wanneer een nieuwe wijziging of taak is voltooid, incheckt bij een gecentraliseerde opslagplaats (Abrantes & Travassos, 2011). CI zorgt ervoor dat het hele ontwikkelteam gesynchroniseerd blijft en het voorkomt de vertragingen veroorzaakt door integratieproblemen (Fowler & Foemmel, 2006; Humble & Farley, 2010). CI is voor de meeste projecten een enorme stap voorwaarts wat betreft productiviteit en kwaliteit. Het zorgt ervoor dat teams samenwerken om zo met meer vertrouwen en controle aan grote en complexe systemen te werken.

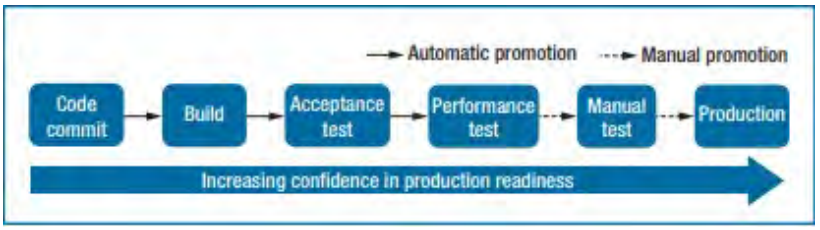
CI zorgt ervoor dat de code die als team is ontwikkeld werkt door het snel geven van feedback over problemen die mogelijk optreden bij het doorvoeren van de betreffende wijzigingen. Het is primair gericht op het feit dat de code succesvol wordt gecompileerd en een aantal unit tests en acceptatietests doorstaat (Humble & Farley, 2010; Olsson et al., 2012). Nadat de ontwikkelaar de laatste wijzigingen heeft ingecheckt, probeert een continu integratiesysteem de broncode te compileren. Als het bouwproces succesvol is afgerond, voert het continue integratiesysteem systeemtests en integratietests uit. Met een build als een object wordt bedoeld een uitvoerbaar artefact samengesteld uit een broncode. Als sommige tests mislukken, informeert het continue integratiesysteem de ontwikkelaar onmiddellijk, bijvoorbeeld via e-mail, welke tests zijn mislukt. Het idee achter CI is om de problemen die optreden bij de integratietestfase zo snel mogelijk op te sporen en de feedback zo snel mogelijk aan de ontwikkelaar te bezorgen (Pulkkinen, 2013). Sommigen hebben dit verder uitgebreid door geautomatiseerde acceptatietests op te nemen. De meest extreme toepassing is die waarbij het gehele proces wordt geautomatiseerd zodat releases automatisch naar productie worden gebracht. Dit wordt 'continuous deployment' genoemd (Pulkkinen, 2013), welke de volgende stap is na 'continuous delivery'.
Stahl en Bosch (2013) beschrijven dat CI populair is bij het ontwikkelen van software onder andere doordat het de releasefrequentie en voorspelbaarheid vergroot. Daarnaast gaat de productiviteit van ontwikkelaars omhoog en verbetert het de communicatie. De output van het CI systeem is normaal gesproken de input voor het handmatige testproces en tevens voor de rest van het releaseproces. Een groot deel van de problemen in het vrijgeven van software ontstaat door belemmeringen tijdens het testproces. Humble & Farley (2010) geven hiervan enkele voorbeelden:

- Ontwikkelteams en beheerteams wachten op documentatie of "fixes"
- Testers wachten op een "goede" build van de software
- Ontwikkelteams ontvangen bug reports weken nadat het team is overgegaan op de nieuwe functionaliteit

Volgens Humble & Farley (2010) is CI slechts de eerste stap. Software dat succesvol in een codestroom is geïntegreerd, is nog steeds geen software dat in productie is en zijn werk doet.

3.1.2 Continuous Delivery

'Continuous delivery' (CD) is een software engineering aanpak waarbij teams software blijven produceren in korte cycli (Krusche & Alperowitz, 2014) en ervoor zorgen dat de software op ieder moment kan worden vrijgegeven naar de productieomgeving (Chen, 2015; Pulkkinen, 2013). Dit kan zijn wekelijks of dagelijks, of het kan betekenen dat iedere check-in rechtstreeks naar productie wordt gebracht. De frequentie van releasen is echter niet de beslissende factor, maar het is de mogelijkheid om te allen tijde te releasen (Neely & Stolt, 2013). CD bestaat uit de CI fase inclusief geautomatiseerde implementatie in testomgevingen voor geautomatiseerde acceptatie en performance tests (Pulkkinen, 2013). Waar CI zicht richt op de automatisering van het ontwikkelproces, breidt CD dit uit met automatisering van testen en implementatie van nieuwe software. CD heeft als doel de release van software te vereenvoudigen en maakt kortere feedbackcycli mogelijk tussen ontwikkelaars en klanten. Naast deze voordelen stelt CD teams in staat de status van de software continu te monitoren, vermindert het integratiefouten en configuratiefouten, vermindert het stress bij het werken met releases en verhoogt het de flexibiliteit van de implementatie (Krusche & Alperowitz, 2014). CD voorstanders beweren dat het organisaties snel, efficiënt en betrouwbaar software op de markt brengt en daarbij een stap voor blijft op de concurrentie die geen gebruik maakt van CD. Chen (2015) maakt hierbij wel de kanttekening dat de implementatie van CD zeer uitdagend kan zijn, vooral voor grotere organisaties die veelal te maken hebben met een bestaande ontwikkelomgeving en productieomgeving.
CD kan ingezet worden voor verschillende applicaties binnen een organisatie. Als basis wordt voor iedere applicatie een CD pipeline opgezet. Deze CD pipeline kan per applicatie verschillen wat betreft het aantal en het type fasen. Het software ontwikkelingsteam dient ervoor te zorgen dat de CD pipeline past bij de eisen van het project (Krusche & Alperowitz, 2014).



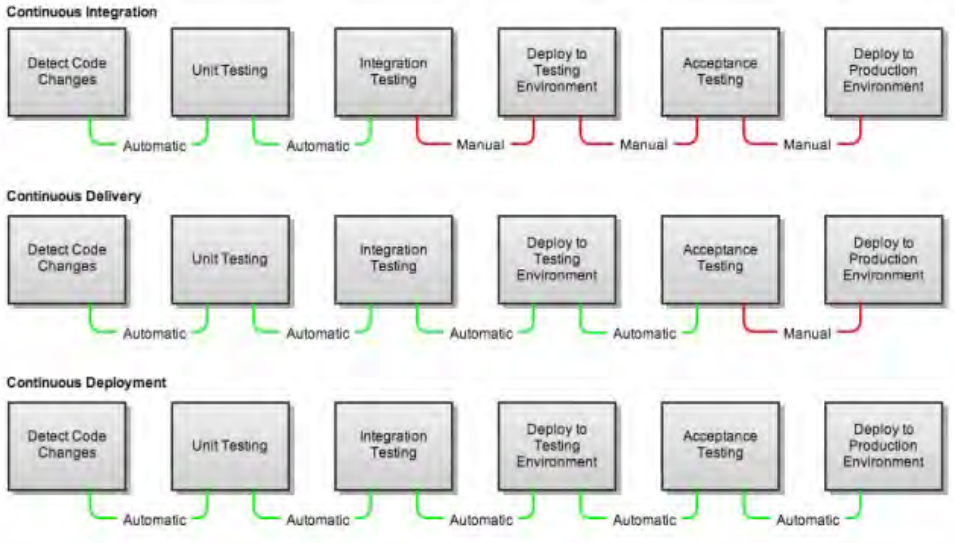
Figuur 1. Voorbeeld van een CD pipeline (Chen, 2015).

De code commit fase geeft direct feedback aan de ontwikkelaar bij het inlezen van de code. Tevens worden er unit tests uitgevoerd. Indien er fouten worden geconstateerd stopt het proces en wordt de ontwikkelaar op de hoogte gesteld. De ontwikkelaar zal in dit geval de code moeten repareren, waarbij wijzigingen een peer review ondergaan en waarna de code opnieuw wordt ingelezen. Wanneer er geen fouten meer worden geconstateerd zal de pipeline automatisch doorgaan naar de volgende fase.
De build fase voert opnieuw de unit tests uit zodat integratie tests en verschillende code analyses kunnen worden uitgevoerd en tevens de vereiste artefacten kunnen worden gebouwd voor de release. Vervolgens worden deze artefacten ingeladen en beheerd in een repository voor in productiename of distributie.
De acceptance test fase zorgt er voornamelijk voor dat de software voldoet aan de specifieke eisen van de gebruiker. De pipeline creëert de acceptance test omgeving, conform de productieomgeving, waarin de nieuwe software is uitgerold. Vervolgens wordt de acceptatie test automatisch uitgevoerd door de pipeline en vereist dit geen manuele handelingen van de ontwikkelaar. Zoals ook in eerder fasen zal, wanneer er geen fouten meer worden geconstateerd, de pipeline automatisch doorgaan naar de volgende fase.
De performance test fase gaat na hoe de code wijziging de software prestaties beïnvloedt. De pipeline creëert een performance testomgeving waarin test worden uitgevoerd en vervolgens de resultaten zichtbaar worden gemaakt in de tool. Ontwikkelaars ontvangen zo direct feedback over in welke mate de wijziging de prestaties beïnvloed en kunnen hier tijdig naar handelen.
Naast de automatische tests kan het nodig zijn om manuele tests uit te voeren. Deze testomgeving wordt ook automatisch gecreëerd door de pipeline. Wanneer deze tests succesvol zijn afgerond worden de artefacten klaargezet voor in productiename. In productiename wordt in gang gezet door een druk op de knop. Doordat het implementatieproces geen manuele handelingen meer vereist, en de scripts meerdere malen zijn getest in eerdere fasen, is de kans op fouten klein.
De technische discipline die vereist is om een dergelijk model te ondersteunen, moet sterk zijn. Systemen moeten nauwkeurig worden afgestemd en uitgebreid worden beheerst door automatisering, met grondige monitoring- en testkaders (Neely & Stolt, 2013). De verbeterde testdekking, snelle feedbackcycli, controle van monitoringsystemen en snelle rollback mechanismen resulteren in een veel veiligere omgeving voor het transporteren van code (Neely & Stolt, 2013).

3.1.3 Continuous Deployment

Het idee achter Continuous Deployment is voortgekomen uit Continuous Integration welke voor het eerst werd gepresenteerd door Martin Fowler in het jaar 2000 (Pulkkinen, 2013). De concepten Continuous Delivery en Continuous Deployment zijn beschreven door Humble & Farley (2010).
Bij Continuous Deployment wordt elke wijziging die de geautomatiseerde tests doorstaat automatisch in de productieomgeving geïmplementeerd. Hierbij moeten alle testfasen volledig worden geautomatiseerd, inclusief acceptatietests die functionele vereisten en niet-functionele vereisten omvat (Pulkkinen, 2013). De software functionaliteit wordt continu, of in hogere frequentie, aan de klantzijde geïmplementeerd. Dit maakt het mogelijk om continue feedback van klanten te ontvangen, te leren van klantgegevens en werk

te elimineren dat geen waarde oplevert voor de klant. Afdeling R&D, productbeheer en de klanten zijn allemaal betrokken bij een snelle, agile cyclus van productontwikkeling (Olsson et al., 2012).

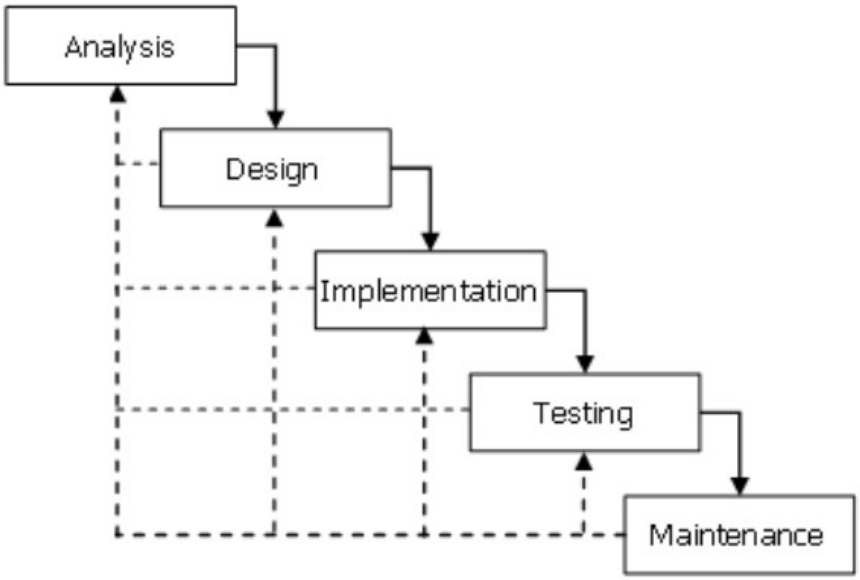


Figuur 2. Continuous Integration, Continuous Delivery, Continuous Deployment (Pulkkinen, 2013).

In figuur 2 worden de verschillen weergegeven tussen de verschillende ontwikkel technieken. Indien een organisatie beperkingen in het proces heeft doordat het compliant dient te zijn met wetgeving en regelgeving, dan zijn goedkeuringen vereist voordat een nieuwe build naar de productieomgeving wordt uitgerold (Humble & Farley, 2010). In dat geval kan de organisatie niet continu nieuwe software uitrollen naar de productieomgeving met behulp van een geautomatiseerde pipeline (Pulkkinen, 2013).

3.2 Stabiele productieomgeving

In de hoofdstukken hierboven hebben we de term DevOps en de daarmee samenhangende ontwikkelmethoden toegelicht. Met deze nieuwe ontwikkelmethoden ontstaan nieuwe risico's en beheersingsdoelstellingen. Voordat in deze scriptie hier nader op wordt ingegaan zal eerst een uiteenzetting worden gemaakt van de risico's en beheersingsdoelstellingen bij het gebruik van de traditionele softwareontwikkelingen, namelijk de Waterval software ontwikkelmethode. De Waterval methode is een softwareontwikkelingsproces waarbij voortgang wordt gemeten aan de hand van fasen die opeenvolgend moeten worden doorlopen.



Figuur 3. Het Waterval model (Bassil, 2012)

De accountantsorganisatie heeft op basis van de Waterval software ontwikkelmethode risico's in kaart gebracht die gepaard gaan met het gebruik van IT en die invloed kunnen hebben op de juistheid en volledigheid van de cijfers op de jaarrekening van een organisatie. In tabel 1 is een weergave gegeven van de risico's (Auditmethodologie accountantsorganisatie, 2018).

	IT process		
Risks of using IT addressed by IT processes	**Manage change**	**Manage access**	**Manage IT operations**
New IT application programs or changes to existing programs do not function as described or requested because they are not adequately tested by appropriate persons other than the developers or aren't appropriate for the business or the IT environment	✓		
Programs in production are not secured permitting developers to move unauthorized or untested changes to the production environment	✓		
Configuration changes made by IT personnel are inappropriate or unauthorized	✓		
Direct data changes made by IT personnel without authorization		✓	
Inadequate authentication and security settings		✓	
Users of the IT environment are not authorized because: Requests for removal of unneeded access of IT personnel are not made timely Access action requests fulfilled inaccurately or untimely		✓	
The access of IT users of the IT environment creates segregation of duties concerns		✓	

Failure to make requested changes to systems or programs			✓
Issues with programs that cannot process to completion are not addressed or are addressed inappropriately			✓
Hardware or software issues result in loss of data or the ability to accurately process that data			✓

Tabel 1. Auditmethodologie accountantsorganisatie

Indien de risico's met betrekking tot het IT proces 'Manage Change', ofwel wijzigingsbeheer, voor een bepaalde applicatie gedurende de audit periode in voldoende mate worden beheerst, kan men spreken van een stabiele productieomgeving.

3.3 Automatiseren van beheersingsmaatregelen

Wijzigingsbeheer, ofwel change management, is het proces van het volgen en monitoren van wijzigingen zodat beheersing behouden kan worden en de technische voortgang wordt begrepen richting het leveren van een acceptabel eindgebruikersproduct (Alger et al., 2009). Hoe minder beheersing we hebben over de omgeving waarin een code wordt uitgevoerd, des te groter het potentieel voor ongewenst gedrag (Humble & Farley, 2010). Met de implementatie van DevOps zullen organisaties dus naar de mogelijkheid moeten kijken om de beheersingsmaatregelen omtrent het wijzigingsbeheerproces te automatiseren.

3.3.1 Testwerkzaamheden

Veel primaire studies benadrukken het belang van het gebruik van testen en kwaliteitsborging (QA) door het hele ontwikkelingsproces in de context van Continuous Delivery, omdat functies worden uitgerold, en niet alleen aan het einde van de ontwikkeling (Rodriguez et al., 2017). Een systematische benadering van testwerkzaamheden is gericht op het maximaliseren van foutdetectie, het reproduceerbaar maken van resultaten en het verminderen van de invloed van externe factoren, zoals willekeurige selectie van testgevallen of de stemming van de tester (Muccini et al., 2012). Te veel projecten vertrouwen uitsluitend op handmatige acceptatietests om te controleren of een bepaald stuk software voldoet aan de functionele en niet-functionele vereisten. Zelfs waar geautomatiseerde tests bestaan, zijn ze vaak slecht onderhouden en verouderd en moeten ze worden aangevuld met uitgebreide handmatige tests (Humble & Farley, 2010).
De traditionele watervalbenadering leidt tot de neiging om verificatie en kwaliteit te beschouwen als afzonderlijke activiteiten, die alleen in overweging kunnen worden genomen nadat vereisten, ontwerp en codering zijn voltooid (Fitzgerald & Stol, 2014). Het belangrijkste aandachtsgebied als het gaat om de implementatie van DevOps is het ontwikkelen van een volledig geautomatiseerde testinfrastructuur die het product tijdens de ontwikkeling voortdurend controleert (Olsson et al., 2014). In testautomatisering wordt een verscheidenheid aan testsuites uitgevoerd, waaronder unit tests, functionele tests, integratie tests en prestatie tests, in verschillende fasen en met verschillende reikwijdte (Humble et al., 2006; Rodriguez et al., 2017). Deze testsuites gebruiken procedures, zoals het automatisch uitvoeren van testscripts op een ontwikkel server, nadat elke code gereed is gemaakt om te testen en om de status van de code of de build te controleren (Rodriguez et al., 2017) en geautomatiseerde acceptatietests (Humble et al., 2006).

Code commit

Met een geautomatiseerde codebeoordeling wordt vastgesteld dat het systeem op technisch niveau werkt. Er wordt een reeks van geautomatiseerde tests uitgevoerd waarbij tevens de code wordt geanalyseerd (Humble & Farley, 2010; Chen, 2015). Fouten kunnen snel worden verholpen, terwijl de context nog vers in de hoofden zit van de ontwikkelaars en voordat deze fouten leiden tot problemen. Ook kunnen de onderliggende oorzaken die hebben geleid tot de problemen worden geïdentificeerd en geëlimineerd ((Fitzgerald & Stol, 2014).
Wanneer er fouten worden geconstateerd wordt de ontwikkelaar op de hoogte gesteld. De ontwikkelaar zal in dit geval de code moeten repareren, waarbij na een peer review van een tweede ontwikkelaar de

code opnieuw wordt ingelezen (Chen, 2015). Het is van vitaal belang dat het ontwikkelteam een gevoel van eigenaarschap heeft voor deze fase. Het is nauw verbonden met hun werk en hun productiviteit. Als er belemmeringen worden opgelegd tussen de ontwikkelaars en hun vermogen om snel en effectief veranderingen aan te brengen, zal hun voortgang vertragen en problemen worden opgeslagen en tot uiting komen later in het proces (Humble & Farley, 2010).
Wanneer een applicatie connecties heeft met verschillende externe systemen, of wanneer de applicatie bestaat uit een reeks los gekoppelde modules met daartussen complexe interacties, dan worden ook integratietests belangrijk. Integratietests zorgen er namelijk voor dat elk onafhankelijk onderdeel van de applicatie op een juiste manier werkt met de services waar het gebruik van maakt (Humble & Farley, 2010). Het doel is om de problemen die zich voordoen bij de integratietestfase zo snel mogelijk op te sporen en de feedback zo snel mogelijk aan de ontwikkelaar te bezorgen (Pulkkinen, 2013).

Geautomatiseerde acceptatietests
Het doel van de acceptatietestfase is ervoor zorgen dat het systeem de waarde levert die de klant verwacht en dat het voldoet aan de specifieke eisen van de gebruiker (Humble & Farley, 2010; Chen, 2015). De acceptatietestfase dient ook als een regressietest omgeving, waarbij wordt geverifieerd of er geen nieuwe bugs worden geïntroduceerd bij aankomende wijzigingen. Indien de code regelmatig moet worden vrijgegeven, zoals bij DevOps, moeten de handmatige stappen worden verwijderd (Neely & Stolt, 2013). Acceptatietests moeten worden geschreven, en idealiter worden geautomatiseerd, voordat het ontwikkelteam start met een wijziging (Humble & Farley, 2010).
Het opzetten van de acceptatie testomgeving kan worden ingeregeld als een automatisch proces waarmee een omgeving wordt opgezet die gelijk is aan de productieomgeving. Dit omvat tevens het opzetten en configureren van servers. Vervolgens wordt hierin de nieuwe software uitgerold. Het opzetten van de acceptatieomgeving is in andere gevallen een handmatige handeling die veel tijd in beslag kan nemen van zowel de ontwikkelaars als de testers (Chen, 2015). Het automatiseren van acceptatietests hebben volgens Humble en Farley (2010) een aantal waardevolle eigenschappen:

- Ontwikkelaars kunnen geautomatiseerde tests uitvoeren om te achterhalen of ze een bepaald vereiste hebben voltooid zonder hiervoor naar de testers te hoeven gaan. De feedback cyclus wordt hierdoor sneller doorlopen.
- Werkdruk op testers wordt verminderd.
- Ze laten testers vrij zich te concentreren op verkennende tests en activiteiten met hogere waarde in plaats van repetitieve taken.
- De acceptatietests vormen een krachtig regressietestpakket. Dit is van belang bij het schrijven van grote applicaties of bij het werken in grote teams waarbij raamwerken of veel modules worden gebruikt en wijzigingen in een deel van de applicatie waarschijnlijk van invloed zijn op andere functies.

Het inzetten van acceptatietesten is een belangrijke toevoeging aan de effectiviteit van het ontwikkelproces. Het dient de aandacht te richten op alle leden van het team op wat echt telt, het gedrag dat de gebruikers van het systeem nodig hebben (Humble & Farley, 2010).

3.3.2 Release op de productieomgeving
Er is een bedrijfsrisico verbonden aan elke release en derhalve willen we controle hebben over elke wijziging die wordt aangebracht op de productieomgeving. De meeste problemen die optreden binnen de productieomgeving van een applicatie worden veroorzaakt doordat de organisatie onvoldoende controle kan uitoefenen op deze productieomgeving. De productieomgeving zal volgens Humble & Farley (2010) volledig afgesloten moeten zijn, waarbij wijzigingen enkel naar productie kunnen worden gebracht door middel van automatische processen. Dit omvat niet alleen de in productiename van een applicatie, maar ook wijzigingen aan de configuratie en het netwerk. Volgens Humble & Farley (2010) is het enkel op deze manier mogelijk om de productieomgeving op een betrouwbare manier te controleren, problemen te herkennen en tijdig op te lossen.

Met het automatiseren van in productiename en release van wijzigingen zullen ontwikkelaars, testers en het beheerteam niet meer hoeven te steunen op het ticketing systeem en email voor het verzamelen van feedback omtrent de gereedheid van het product (Humble & Farley, 2010). In productiename wordt in gang gezet door een druk op de knop (Chen, 2015). Een belangrijke reden voor het verminderen van het risico is de mate waarin het proces van releasen zelf wordt herhaalt, getest en geperfectioneerd. Aangezien hetzelfde proces wordt gebruikt om wijzigingen naar productie te brengen, wordt het implementatieproces zeer vaak getest (Humble & Farley, 2010; Chen, 2015). Een ander potentieel voordeel van het automatiseren van het release proces is dat het een snelle cyclustijd mogelijk maakt, waaronder ook het repareren van bugs of patches (Anderson et al., 2014).

4 Resultaten

Gedurende een periode van twee weken zijn er zes gesprekken gevoerd met verschillende medewerkers, hierna genoemd 'Experts', binnen één van de grootste energieleveranciers van Nederland. De medewerkers dragen de volgende functies: Manager Agile Delivery, Medewerkers Agile IT, Tester, Product Owner en Developer.
Tijdens deze gesprekken is besproken hoe de organisatie DevOps heeft ingericht, welke risico's hiermee gepaard gaan en welke beheersingsmaatregelen zijn ingericht om deze risico's te mitigeren. Volgens de experts heeft DevOps binnen de organisatie een aantal kenmerken, namelijk:

- Nadat wijzigingen zijn ontwikkeld, worden deze automatisch gemigreerd naar de volgende omgeving (QA & UAT) om geautomatiseerde of manuele testscripts te ondergaan.
- Goedgekeurde wijzigingen worden manueel naar productie gebracht, of middels een geautomatiseerde tool.
- Ontwikkelaars en beheerders zijn getraind en krijgen toegang tot alle omgevingen voor ondersteuning en het oplossen van problemen op elk gewenst moment in het software ontwikkelproces.

De change management risico's bij het gebruik van DevOps blijven gelijk aan die van de traditionele Waterval methodiek, echter zullen er additionele beheersingsmaatregelen moeten worden opgesteld. In onderstaand overzicht zijn per risico de additionele overwegingen opgenomen welke volgens de experts aandacht zouden moeten krijgen bij het gebruik van DevOps.

IT proces risico's	Additionele overwegingen
New IT application programs or changes to existing programs, including reports, configurations and interfaces, do not function as described or requested because they are not adequately tested by appropriate persons.	- Het begrijpen van de diepgang van het testen en goedkeuringen in de ontwerp, bouw en testfase, waar deze worden bewaard en door wie. o Goedkeuringen kunnen worden vastgelegd per wijziging of tijdens een periodieke vergadering. - Versiebeheer nauwlettend in de gaten houden. Vanwege de toegenomen frequentie en het grotere aantal wijzigingen kunnen er meerdere builds bestaan voor een wijziging. Bewijzen voor testen, goedkeuring en in productiename zal volledig en nauwkeurig in kaart moeten worden gebracht voor de versie die wordt gebruikt in de productieomgeving.
New IT application programs or changes to the production IT application programs (including reports and interfaces) are not appropriate for the business or the IT environment.	

	- DevOps kan het moeilijker maken om de ontwikkelde software te reviewen op security of coding fouten. o Geautomatiseerde software scans en vulnerability scans tijdens het release proces kunnen fouten opsporen zonder het software ontwikkel proces te onderbreken.
Programs in production are not secured permitting developers to move unauthorized or untested changes into the production environment.	- Compenserende maatregelen om het risico aan te pakken dat ontwikkelaars en beheerders toegang hebben tot Dev, QA en productieomgevingen. o Voorbeeld is dat er voor iedere wijziging een log wordt aangemaakt zodat deze kan worden aangesloten met de wijziging, zodat iedere aanpassing kan worden gerelateerd aan een wijziging.
Configuration changes made by IT personnel are inappropriate or unauthorized.	
Multiple instances of the same IT application that should be identical are not the same.	- Beoordelen in welke mate de organisatie steunt op geautomatiseerde tools. Wanneer tools worden gebruikt om configuraties in meerdere instances te beheren, is het van belang om de besturingselementen die zijn ontworpen om dit proces te beheren te beoordelen.

Tabel 2. Additionele overwegingen DevOps

In aanvulling op bovenstaande additionele overwegingen is het volgens de experts tevens van belang dat ontwikkelaars training krijgen op het gebied van security. Dit omdat het pad van softwareontwikkeling naar productie is geautomatiseerd en kwetsbaarheden in dit proces moeten worden voorkomen.

5 Discussie en implicaties

Het doel van deze scriptie was het onderzoeken van de maatregelen die genomen moeten worden om een stabiele productieomgeving te realiseren bij het gebruik van DevOps. Als resultaat zijn de additionele overwegingen weergegeven per IT risico welke volgens de experts aandacht zouden moeten krijgen bij het gebruik van DevOps.
Omdat de frequentie en het aantal wijzigingen toenemen bij DevOps impliceren de resultaten dat het belangrijk is de diepgang te begrijpen van de testwerkzaamheden in iedere fase binnen het ontwikkelproces. Bewijzen voor testen, goedkeuring en in productiename zal volledig en nauwkeurig in kaart moeten worden gebracht voor de versie die wordt gebruikt in de productieomgeving. Deze resultaten zijn in lijn met het literatuuronderzoek, echter laat het tevens zien dat het moment van goedkeuren afhangt van of de organisatie in productiename heeft geautomatiseerd.
De resultaten geven verder aan dat DevOps het moeilijker kan maken om de ontwikkelde software te reviewen op security of coding fouten. Geautomatiseerde software scans en vulnerability scans tijdens het release proces kunnen fouten opsporen zonder het software ontwikkelproces te onderbreken. Een tekortkoming van het huidige literatuuronderzoek is dat de focus ligt op het wijzigingsbeheer en derhalve security onderbelicht blijft. Additioneel onderzoek zal moeten uitwijzen in welke mate security risico's gepaard

gaan met DevOps en welke beheersingsmaatregelen ingericht kunnen worden om deze risico's te mitigeren.
Daarnaast zullen er, volgens de resultaten, compenserende maatregelen moeten worden ingericht om het risico aan te pakken dat ontwikkelaars en beheerders toegang hebben tot de ontwikkelomgevingen, testomgevingen en productieomgevingen. Dit is in lijn met het literatuuronderzoek, waarin een review op de logging wordt beschreven na implementatie van iedere wijziging. Een betrouwbare audit trail is derhalve een vereiste in het kunnen garanderen van een stabiele productieomgeving bij het gebruik van DevOps.
Als laatst gaan de resultaten in op het risico van geautomatiseerde tools. Wanneer tools worden gebruikt om configuraties in meerdere instances te beheren, is het van belang om de besturingselementen die zijn ontworpen om dit proces te beheren te beoordelen. In het literatuuronderzoek wordt niet specifiek ingegaan op geautomatiseerde tools, wel beschrijft het beheersingsmaatregelen die als zodanig kunnen worden geïnterpreteerd.

5.1 Contributie en implicaties

Door het identificeren van belangrijke overwegingen die gemaakt dienen te worden bij het gebruik van DevOps, geeft deze scriptie theoretisch inzicht in de factoren en beheersingsmaatregelen die een rol spelen in het realiseren van een stabiele productieomgeving. Resultaten uit deze scriptie kunnen organisaties helpen bij het begrijpen van DevOps risico's en hoe deze risico's af te dekken met de juiste beheersingsmaatregelen om zo een stabiele productieomgeving te realiseren. Het conceptueel model in deze scriptie kan worden toegepast in verschillende industrieën om zo de toepasbaarheid in verschillende contexten te beoordelen.
Vanuit een praktisch perspectief heeft deze scriptie implicaties voor organisaties die DevOps gebruiken, of gaan gebruiken, in het software ontwikkelproces. Als eerst laten de resultaten zien dat testwerkzaamheden geautomatiseerd worden. Derhalve zullen organisaties de diepgang van de testwerkzaamheden moeten begrijpen en deze beoordelen. Wanneer geautomatiseerde tools worden gebruikt is het van belang om de besturingselementen die zijn ontworpen om dit proces te beheren te beoordelen.

5.2 Tekortkomingen en toekomstig onderzoek

Zoals reeds eerder besproken ligt de focus van het huidige conceptueel model op wijzigingsbeheer en derhalve blijft security onderbelicht. Het conceptueel model in deze scriptie is namelijk vooral gericht op assurance en de daarbij behorende stabiele productieomgeving. Toekomstig onderzoek zou zich tevens kunnen richten op governance en security.
Verder is het op te merken dat, omdat DevOps zo sterk afhankelijk is van automatisering, geautomatiseerde benaderingen van het verkrijgen van zekerheid interessanter worden voor organisaties. Meer in het bijzonder kunnen organisaties die zijn overgestapt op 'continuous auditing' of overwegen over te stappen naar continuous auditing, vinden dat integratie van bestaande continue auditmechanismen met DevOps eenvoudiger blijkt dan voor organisaties die strikt handmatige methoden gebruiken. Toekomstig onderzoek zou zich derhalve kunnen richten op DevOps in combinatie met continuous auditing en continuous monitoring.

6 Conclusie

De resultaten in deze scriptie laten zien dat de kenmerken die DevOps aantrekkelijk maken voor organisaties kunnen zorgen voor het verkrijgen van assurance. De veranderende omgeving die gepaard gaat met de adoptie van DevOps kunnen potentieel impact hebben op de bestaande beheersomgeving van de organisaties en het geaccepteerde risico niveau.
Zoals met de meeste nieuwe technologieën is er een bijbehorend risico met de adoptie van DevOps. Voor organisaties kan de kortere cyclustijd die vereist is voor het vrijgeven van applicaties en het toegenomen gebruik van automatisering, direct van invloed zijn op de beheersingsmaatregelen door een toename in de

complexiteit. Met name de impact op de beheersmaatregelen op het gebied van functiescheiding zullen veranderingen teweeg brengen in het benaderen en mitigeren van risico's binnen organisaties.
De maatregelen die genomen moeten worden om een stabiele productieomgeving te realiseren bij het gebruik van DevOps is volgens de resultaten in deze scriptie een combinatie van 'klassieke' beheersingsmaatregelen en 'nieuwe' beheersingsmaatregelen. De nieuwe beheersmaatregelen zijn hierbij specifiek gericht op het mitigeren van de risico's die gepaard gaan met de automatisering van de zogeheten 'deployment pipeline' en het gebruik van geautomatiseerde tools. Een betrouwbare audit trail is hierbij een vereiste in het kunnen garanderen van een stabiele productieomgeving bij het gebruik van DevOps.

7 Referenties

Abrantes, J. F., & Travassos, G. H. (2011, September). Common agile practices in software processes. In Empirical Software Engineering and Measurement (ESEM), 2011 International Symposium on (pp. 355-358). IEEE.

Alger, J., Gvalog, F. J., Wright, L., Arora, R., Rajasekhar, R. N., & Varma, S. (2009). U.S. Patent No. 7,574,483. Washington, DC: U.S. Patent and Trademark Office.

Anderson, K. H., Kenyon, J. L., Hollis, B. R., Edwards, J., & Reid, B. (2014). U.S. Patent No. 8,677,315. Washington, DC: U.S. Patent and Trademark Office.

Bass, L., Weber, I., & Zhu, L. (2015). DevOps: A Software Architect's Perspective. Addison-Wesley Professional.

Bassil, Y. (2012). A simulation model for the waterval software development life cycle. arXiv preprint arXiv:1205.6904.

Chen, Lianping. "Continuous delivery: Huge benefits, but challenges too." IEEE Software 32.2 (2015): 50-54.

Dyck, A., Penners, R., & Lichter, H. (2015, May). Towards definitions for release engineering and devops. In Release Engineering (RELENG), 2015 IEEE/ACM 3rd International Workshop on (pp. 3-3). IEEE.

Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). DevOps. IEEE Software, 33(3), 94-100.

Fitzgerald, B., & Stol, K. J. (2014, June). Continuous software engineering and beyond: trends and challenges. In Proceedings of the 1st International Workshop on Rapid Continuous Software Engineering (pp. 1-9). ACM.

Fitzgerald, B., & Stol, K. J. (2017). Continuous software engineering: A roadmap and agenda. Journal of Systems and Software, 123, 176-189.

Fowler, M., & Foemmel, M. (2006). Continuous integration. Thought-Works) http://www. thoughtworks. com/Continuous Integration. pdf, 122, 14.

Hüttermann, M. (2012). DevOps for developers. Apress.

Humble, J., & Farley, D. (2010). Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation (Adobe Reader). Pearson Education.

Humble, J., Read, C., & North, D. (2006, July). The deployment production line. In Agile Conference, 2006 (pp. 6-pp). IEEE.

Kim, G. (2013). Top 11 things you need to know about DevOps.

Krusche, S., & Alperowitz, L. (2014, May). Introduction of continuous delivery in multi-customer project courses. In Companion Proceedings of the 36th International Conference on Software Engineering (pp. 335-343). ACM.

Labs, P., and Revolution IT. 2015 State of DevOps Report (2018). Opgevraagd 7 Maart, 2018, van https://puppetlabs.com/sites/default/files/2015-state-of-devops-report.pdf

Moyle, M. (2015). Devops: Practitioner Considerations. ISACA.

Muccini, H., Di Francesco, A., & Esposito, P. (2012, June). Software testing of mobile applications: Challenges and future research directions. In Proceedings of the 7th International Workshop on Automation of Software Test (pp. 29-35). IEEE Press.

Neely, S., & Stolt, S. (2013, August). Continuous delivery? easy! just change everything (well, maybe it is not that easy). In Agile Conference (AGILE), 2013 (pp. 121-128). IEEE.

Olsson, H. H., Alahyari, H., & Bosch, J. (2012, September). Climbing the" Stairway to Heaven"--A Mulitiple-Case Study Exploring Barriers in the Transition from Agile Development towards Continuous Deployment of Software. In Software Engineering and Advanced Applications (SEAA), 2012 38th EUROMICRO Conference on (pp. 392-399). IEEE.

Pulkkinen, V. (2013). Continuous deployment of software. In Proc. of the Seminar (Vol. 58312107, pp. 46-52).

Ståhl, D., & Bosch, J. (2014). Modeling continuous integration practice differences in industry software development. Journal of Systems and Software, 87, 48-59.
Technologies, CA. DecOps: The Worst Kept Secret to Winning in the Application Economy (2016). Opgevraagd 6 Maart, 2018, van https://www.ca.com/content/dam/ca/us/files/white-paper/devops-winning-in-application-economy-2.pdf
The Science of DevOps Decoded (2016). Opgevraagd 6 Maart, 2018, van https://www.gartner.com/smarterwithgartner/the-science-of-devops-decoded/

Ur Rahman, A. A., & Williams, L. (2016, April). Security practices in DevOps. In Proceedings of the Symposium and Bootcamp on the Science of Security (pp. 109-111). ACM.

Reframing Security in Contemporary Software Development Life Cycle

Pieter Frijns
Robert Bierwolf
Tom Zijderhand

Dr. Pieter Frijns
Bureau Gateway
Ministry of Interior
The Hague, The Netherlands
pieter.frijns@minbzk.nl

Robert Bierwolf, MScEng. SMIEE
MBBI bv, IEEE TEMS
Utrecht, The Netherlands
robert.bierwolf@xs4all.nl; robert.bierwolf@ieee.org

Tom Zijderhand, BSc.
Deloitte Risk Advisory B.V
Deloitte Touche Tohmatsu Limited
Amsterdam, The Netherlands
tzijderhand@deloitte.nl

1 Introduction

The digital transformation of society is continuing at a faster pace than ever, exponentially, where information technology (IT) has become the business, enabled by technology and triggered by the ongoing disruptive innovation, impacting organizations in their technology management and operations [1].
Ever more organizations are dependent on each other for realizing their goals, eco-systems emerge. From structural partnerships (e.g., joint ventures, tier 1 supplier) to more often as temporary collaborations for the duration of the intended joint result (e.g., consortia). Hence, an increased dynamically networking society is emerging, the volatile-uncertain-complex-ambiguous (VUCA) world, requiring adapted approaches [2]. Resilience becomes essential, e.g., in a just-in-time supply chain network [3], demanding flexibility from people and organizations. Agility in the organizational perspective, is described as: "an agile organization (designed for both stability and dynamism) is a network of teams within a people-centred culture that operates in rapid learning and fast decision cycles which are enabled by technology, and that is guided by a powerful common purpose to co-create value for all stakeholders." [4]. Which impacts IT development and management processes to fit these needs and dynamics, e.g., using Agile Scrum [5], [6] and DevOps [7], [8] in the software development life cycle (SDLC) [9], [10].
With the increasing digitization rate, fast-growing digital data, and communication links between systems and organizations, the number of security risks is also increasing [11]. Author experiences in and from IT Audit reveal that security aspects are not as frequently taken into account as it should be in these digitalizing organizations, e.g., as imposed by such standards as ISO 27000 series [12].
Questions that emerge are to what extent: [a] is or should and could this feature of security be embraced by the product owners and addressed in the approaches such as Agile and DevOps and how could it be managed? ; [b] is the noted insufficient adoption due to the behaviour professional or an inherent limitation of the approaches?; [c] the general question is to what extent these new approaches of Agile and DevOps support, at all or by design, the needs due to the ongoing digitalisation as well as the increasing demands on security?
In the first section of the paper, the concepts are presented of Agile Scrum and Devops and security. The second section, reports the findings of the initial desk research. The desk research comprised a comparing the concepts of Agile and DevOps, along the phases of the SDLC, using the Open Software Assurance Maturity Model [13] as a measure, and the Lucky Clover Model [14] to address the soft- and hard factors, in terms of Content, Process, Relation and Culture, which lead to a new framework.

2 The Concepts

The desk research used some existing concepts or frameworks, such as the Software Development Life Cycle, Agile Scrum, DevOps and Security based on OpenSAMM.

2.1 Digital transformation and software development

Developing software the traditional way in today's world might have severe consequences for organizations, such as their existence. Bean states that in the coming years organizations have to adopt the Agile way of working and evolve or face the consequences of being eaten [15]. For organizations to survive they require to develop quality software in rapid speed, while having a short time to market and ensuring minimum resource usage and waste. Moreover, the project management of such development projects should not be performed on pre-determined requirements and results but on the continuously changing and evolving customer needs.
Security within Agile software development will become equally important in this digital era, where customers highly value and will require more secure services as well as compliance with legal obligations which are rapidly becoming strict. Due to the fast-paced development of software and the absence of traditional set milestones for security testing, we ask ourselves the following questions:

- How will we guarantee actual user access with such as fast-paced software development environment?
- How is security warranted in the use of the software based products and services created through said software development process?
- What does this mean to the security policies, frameworks and approaches of the organization who adopt the new Agile way of working?
- How is security baselined or anchored within the most used agile way of working, Agile Scrum, and the newest and promising way of agile working, DevOps?

Before presenting the studies, we describe in brief the basic elements of Agile Scrum and DevOps. The primary focus of this paper is on the software development and maintenance process and not so much on the exploitation phase of the software based products and services.

2.2 Agile Scrum

Agile Scrum is a process framework for software development, delivery, and maintenance of complex products [16]. Scrum was already used in the 90's, mostly in IT environments. Agile Scrum aligns with the four main principles from the 2001 Agile Manifesto [17]:

- Individuals and interactions over processes and tools;
- Working software over comprehensive documentation;
- Customer collaboration over contract negotiation;
- Responding to change over following a plan.

Agile is an approach, not a tool or a method. A method is a structured process, a tool is technical and can, for example, be used to automate certain parts of a process. In practice, several tools and methods can be chosen from and are used to implement the Agile approach for any (part of) an organization. The most frequently used method is Agile Scrum [18].

2.3 DevOps

DevOps is a term which came to life in 2009 by Patrick Debois when he hosted the event named: The DevOpsDays. DevOps does what the name implies, integrating software development and software operation departments as one. Thus, DevOps acknowledges the interdependencies between both development and operations and integrates these to ensure, in theory, that the organization can produce software faster for deployment to the live production environment without losing service stability and flexibility. The DevOps speed and flexibility has as a goal to support innovation [7].

To assure the innovation, parts of the SDLC circle can be automated. Automation within the SDLC reduces the outstanding workload and prevents errors and ensures that the applications work as expected. The DevOps Handbook describes DevOps as a logical consequence of the progression of the agile development approach over the years. DevOps also aligns with aforementioned four main Agile principles from the Agile Manifesto. Moreover, it also uses several value streams from Lean Six Sigma which are the following [19]:

- The manufacturing value stream which has as goal to reduce outstanding workload
- The technology value stream which has a goal to translate the business hypothesis to technology

Agile Scrum and DevOps are focused on software development respectively software maintenance. Security should be taken into account during each phase of software development and maintenance to ensure that possible security flaws are found as early as possible in the process. Security flaws found early in the process are generally easier to solve and significantly cheaper compared to later SDLC stages, similarly and in line to any other bug fixes in software development as some time ago stated by Boehm [20] and as further supported by Dawson [21], recommending Secure SDLC where an IT product is one with security built in rather than security retrofitted.

2.4 Security

Frequently, information security gets associated with the triad terms Confidentiality, Integrity, and Availability and as acronym CIA as outlined in the standard ISO/IEC 27000:20133. CIA implies that security measures must be taken to ensure that for all the formats of information, these aspects are safeguarded on a proper level.

In literature a variety of definitions, methods and tools for measuring security is available. In the current paper security is defined as: " The way in which security is ensured within the various phases of the SDLC". To be able to measure the security the widely adopted Open Software Assurance Maturity Model (Open SAMM) is being used. as well as extra organization culture pattern additions from Deloitte4 as used in practice.

Open SAMM divides SDLC cycle into four business functions, governance, construction, verification and deployment. These four business functions have each three categories with security practices as shown in Fig. 1. The security practices each contain multiple aspects, these underlying security aspects will be used to measure the way security is safeguarded in both Agile Scrum and DevOps.

The first step to answer the general question of this paper was to study the relationship between Agile, DevOps and the software development lifecycle. The results of this desk research are presented in the next section.

3 Initial Findings of the Studies

3.1 Study 1 - Agile Scrum and DevOps relationship to Software Development Lifecycle

Information provisioning has four components to enable people to execute their roles and responsibilities properly and to let the organization function and realize their goals. These four components are: connectivity, hosting, application functionality and devices. This article focuses on the application functionality which is designed by software and is part of the SDLC.

The SDLC is a process to design, develop, test and implement software. It helps to convert requirements into actual software products and features. As the term states, the SDLC is a lifecycle, and can therefore be applied as a continuous process to build, improve and maintain software. Since the SDLC in essence delivers on a company's strategy, the SDLC process should align with the company's strategy, short term goals and priorities. The products and features shipped via the company's SDLC should directly contribute to the overall strategy and goals.

In this new dynamic era of digitalization with more and faster developments than ever before, the need to develop software faster and more innovative is paramount. The software must enable the users to accomplish their tasks more efficiently and effectively aligned with the dynamics and pace that the outside world demands. Regardless of the outside world demands, the basic SLDC principles and phases are still valid: from the moment there is an idea or requirement, the stages of it being developed, implemented and later on decommissioned.

Agile Scrum is currently the most used approach [18] and DevOps is a promising approach which is being adopted with rapid speed. Agile Scrum covers the project phase of the SDLC and DevOps the maintaining and continuously adapting/developing of the developed software during the project phase. On a high abstraction level Agile Scrum and DevOps can be seen as one SDLC circle with Agile Scrum starting off with requirement setting till implementation and verification and DevOps starting from maintain as shown in Fig. 2. DevOps however will, within the maintenance part, always have its own smaller SDLC circles for continuous improvements of the software until the software is decommissioned.

[1] https://www.iso.org/isoiec-27001-information-security.html

[2] Whereas Deloitte specific references have been used for the study, due to corporate intellectual proprietary reasons, no further details or references are presented in the current paper.

The conclusion or result of the first study is that Agile Scrum and DevOps have been placed into the SDLC as shown in Fig. 2 and security therein is measured using the aspects from Open SAMM, together forming the framework for the next step of research conducted.

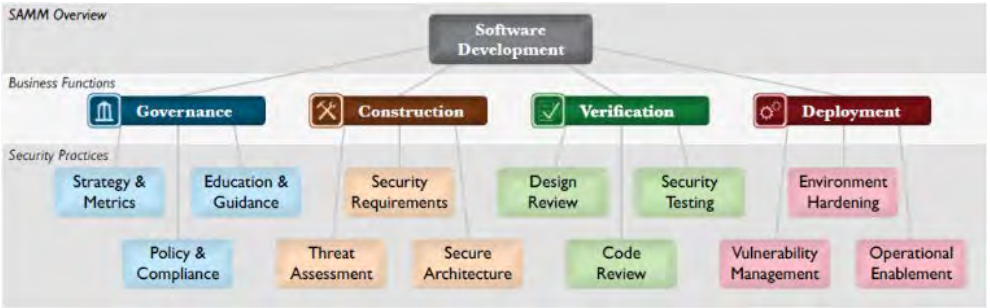


Fig. 1. OWASP, Security & Development Map

3.2 Study 2 - Security related to Agile scrum and DevOps

Based on the theoretical frame as described in Fig 2. , a second study was conducted. The aim of this second study was to analyse the manner in which security is embedded in both Agile Scrum as well as the DevOps approach. To investigate the manner or level of embedding of security in the Agile Scrum and DevOps approaches, the Lucky Clover model was used [2]. The Lucky Clover model was successfully applied in a research on the usability and effectiveness of Agile Scrum and DevOps [22],[23]. The Lucky Clover was further selected and used because it embraces the concepts of the so-called hard and soft aspects. The right leaves of the Lucky Clover relates to hard aspects and the left leaves to soft aspects. As such the inherently present hard and soft aspects of security in both approaches Agile Scrum and DevOps can systematically be investigated and plotted on the Lucky Clover. Cultural and relational aspects are paramount to have a functioning Agile work environment for both Agile Scrum and DevOps. Other organizational models, such as the People-Process-Technology model do not emphasize these prerequisites sufficiently where the Lucky Clover model states these explicitly.

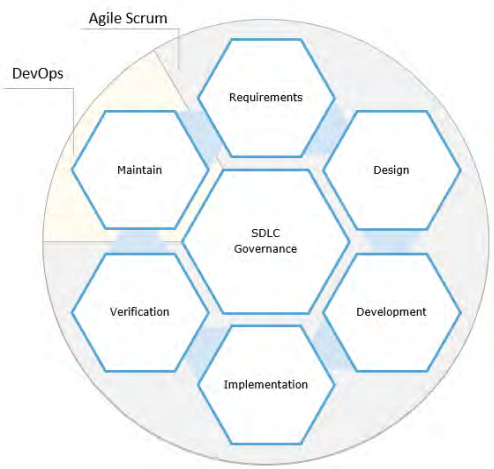


Fig. 2. SDLC, Agile Scrum and DevOps Framed

The results of the initial investigation on security safeguarding and cultural aspects for Agile Scrum are plotted on the Lucky Clover (Fig. 3), which shows that within Agile Scrum the coverage of security aspects within Content and Process are absent. Security is theoretically not guaranteed in the Agile Scrum approach, besides a partly coverage during the design phase of the SDLC.
The cultural aspects of security are important since shared values and behaviour are important aspects. However, the Agile Scrum approach are more or less focused on process aspects while the soft factors are at least as important. In practice an optimal balance between business aspects and technical aspects is needed to be in control on security risks.
Similarly, a mapping for DevOps and security aspects are plotted on the Lucky Clover (Fig 4.), where we observed that on the Content leaf, DevOps covers two out of the six phases completely. What stands out is that mostly the later in life cycle stages Deployment and Verification are embedded and the first stages are not. Three out of six SDLC phases are covered in the Process leaf of the clover, including the overarching governance and one of the first phases of the SDLC.
The conclusion or result of the second study is that Agile Scrum and DevOps have close relations with the Agile Manifesto for Software Development and are both compatible with the Agile approach. In addition DevOps describes several Lean principles in its approach. Several principles match with one approach and the other, such as trust aspects which is deemed paramount within both approaches. Three highlighted comparisons are:
Scrum in particular describes the need of transparency to the accountable person where DevOps describes that everyone is accountable for the product and information should be available for everyone.
DevOps states that a safe learning environment and the possibilities to make mistakes is of high importance whereas Agile Scrum does not attach any value in this area.
DevOps describes the importance of self-managing teams and transparency and trust within the teams. Within the standard Agile Scrum approach relies more on management versus of self-managing.
Summarizing study 2, we may state that security is not covered by the Agile Scrum approach and partly covered within the DevOps approach. Neither of the two approaches cover the aspects within the first phases of the SDLC and DevOps covers several in the later stages but not more than five out of twelve combined phases. The conclusion is that there is insufficient focus is on “Cultural” aspects while shared values as well as the balance between business and technical solutions is needed to be in control. This is in line with the findings on the “Relational” aspects.

3.3 Study 3 – Mapping Agile Scrum, Devops and OpenSAMM with the Lucky Clover

To understand the fundamental factors of these results, a third two-step study was conducted to analyse both Agile Scrum and DevOps approaches in relation to security (OpenSAMM) in more depth.

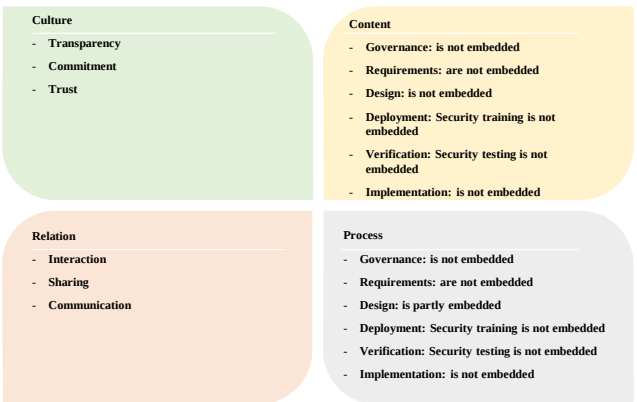


Fig. 3. Agile Scrum and Security Plot on Lucky Clover

This meant doing at first an in-depth analysis regarding the hard aspects “Content” and “Process”, in relation to the Open SAMM security and development phase aspects and Deloitte organization culture patterns. So firstly the security aspects of Agile Scrum and DevOps are plotted in more detail on these two hard aspects.

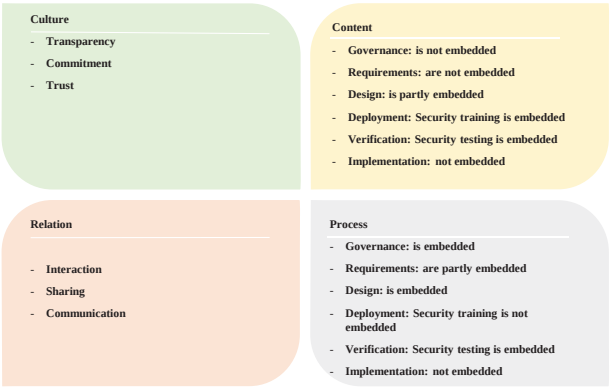


Fig. 4. DevOps and Security Plot on Lucky Clover

When comparing the hard factors in both Agile Scrum and DevOps per SDLC phase the following can be stated:

- Within the Governance phase security aspect coverage is lacking in both Agile Scrum and DevOps
- During the Requirements phase security receives little attention within DevOps and none within Agile scrum
- The Design phase receive both within Agile Scrum some security attention and within DevOps it receives broad attention. In particular on technical level DevOps describes certain requirements such as code review
- Development itself receives minimum attention within Open SAMM, it describes that the development phase is based on skills from employees and thus trainings. DevOps describes such security trainings where Scrum does not.
- The verification phase where testing takes place receives no attention within Agile Scrum. DevOps on the other hand fully complies with Open SAMM and states ever more than the set security aspects. It also describes the need of automation and what effect it might have on the security level of the organization.
- The Maintaining phase is not described within Agile Scrum, DevOps describes it partly and in particular it expresses the needs of rigid vulnerability management to be able to learn from past mistakes.

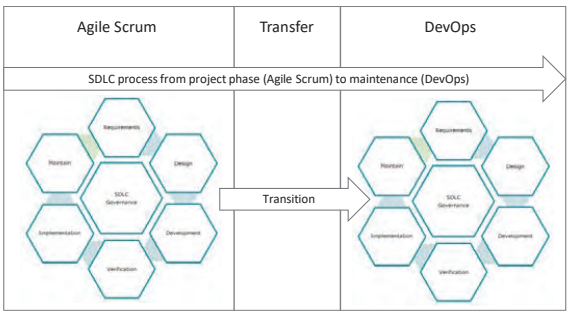


Fig. 5. Connecting Agile and DevOps coherently

The second step concerned the soft aspects: “Relation” and “Culture”, where the security aspects of Agile Scrum and DevOps are plotted in more detail on these two soft aspects. The results thereof are presented in a tabular format, as opposed to being depicted on the Lucky Clover (see Table 1).
When comparing the cultural and relational aspects of both Agile Scrum and DevOps one might state the following:

- Cultural aspects are more taken into account in the DevOps approach.
- In both approaches cultural aspects are underestimated.
- Cultural aspects on shared value and behavioural aspect is not really operationalized.
- The words used referring to cultural aspects are more or less process vocabulary.

4 Conclusion

Security is not like a sauce one can poor over the dinner at the last instance. Embracing security-by-design has become more relevant in the continuing digitalization of society, on software-based products and services and therefore on the development and maintenance cycle. The current paper showed that due to the large differences between Agile Scrum and DevOps issue are inevitable, when developing new software using Agile Scrum and when moving out of the project phase to a live DevOps production and maintenance environment. One might say that the large differences between both approaches increase the likelihood of mistakes, security issues and miscommunication substantially. DevOps relies on different cultural principles and other technical solutions such as automation. If these both of these aspects have not been taken into account during development then going to production might become cumbersome. As Patrick Debois once stated: “Despite all the great methodologies we have in IT, delivering a project to production still feels like going to war” [24].
The problem and challenge to transfer software development from an Agile Scrum approach to a DevOps environment is visualized in Fig.5, showing the coherence of both Agile Scrum and DevOps. This gap requires specific attention to be sure that security aspects are fully covered during transition and even security aspects are enriched during transition.
More important, traditionally security is or has not been an integral part of widely used frameworks for software development. Security is often seen as one of the features or requirements that are required. The fact that security is not a main element in the Agile or DevOps approach is not strange. Given the importance though and impact of security in software nowadays, the recommendation is made that security cannot be seen as a feature but must be an inherent part of the software development approach in line with [20], [21] . Secondly, we conclude that not only the hard controls (Content and Process) should be taken into account, also soft controls (Relations and Culture) should be in focus in a balanced way in line with [14]. With the increasing growth of complexity in the VUCA world, with the proliferation of IoT, security is not the responsibility of just a single person, e.g. the developer or architect, but of the whole development team or ecosystem they are part of, to embrace security-by-design and to ensure it is part of the MVP.
Future research has started to gain more insight on the SDLC security coverage, using the Lucky Clover as framework, within medium and large size enterprises globally. Special attention will be paid to the relational and cultural aspects. Thus, the next step is to research the security behaviour and attitude level of the people, organisations and ecosystems: The important human factor of security.
Clearly, a limitation of the current paper is that this has been a desk research to-date. The next step will be to obtain empirical data from the field in an international setting based on the formats of tables for guiding an inquiry amongst practitioners and organizations.

Lucky clover leaf: Culture	
Cultural aspects Agile Scrum	Cultural aspects DevOps

Transparency to those responsible for the outcome	High level of confidence
Commitment and focus on the goal of the sprint and the scrum team	High transparency, everything is measured and recorded which is clear to everyone
Have the courage to do the right things and work on complex problems	Safe learning environment for everyone
Trust that your team members are capable and independent	Encourage the sharing of knowledge and experience
Openness of the team and the stakeholders about the work and the challenges	Autonomous teams
Responding to change above following a plan	Openness of the team and the stakeholders about the work and the challenges
	Working software above all-encompassing documentation
	Responding to change above following a plan
Lucky Clover leaf: Relation	
Relational aspects Agile Scrum	Relational aspects DevOps
Openness about the work and the challenges	Shared responsibility between team members
Multidisciplinary teams	No silos
	High transparency, everything is measured and recorded which is clear to everyone
trust that your team members are capable and independent	High level of trust both within and within the organization
People and their mutual interaction over processes and tools	Continuous involvement of the business
Collaboration with the customer over contract negotiations	Safe learning environment for everyone
	Solve issues when they appear by Having short and effective feedback loops.
	Solving problems with whoever can get new knowledge as quickly as possible
	Multidisciplinary teams

Table 1: Agile Scrum and DevOps vs Culture and Relation

5 References

[1] M. Poppendieck, “The End of Enterprise IT,” Lean Essays, 2017. [Online]. Available: http://www.leanessays.com/. [Accessed: 20-Sep-2017].

[2] R. Bierwolf, P. Frijns, and P. van Kemenade, “Lifelong learning and dialogue in a VUCAWorld,” IEEE Eng. Manag. Rev., vol. 45, no. 3, pp. 19–24, 2017.

[3] H. Frederiksson and M. Glas, “Operational Disturbances in Supply Management,” Jönköping University, 2012.

[4] W. Aghina, K. Ahlbäck, A. De Smet, C. Fahrbach, C. Handscomb, G. Lackey, M. Lurie, M. Murarka, O. Salo, E. Seem, and J. Woxholth, “The 5 Trademarks of Agile Organizations,” McKinsey&Company, pp. 1–22, Dec-2017.

[5] Agile Alliance, “Agile Manifesto - Manifesto for Agile Software Development,” The Agile Manifesto, 2001. .

[6] B. Hobbs and Y. Petit, “Agile Methods on Large Projects in Large Organizations.,” Proj. Manag. J., vol. 48, no. 3, pp. 3–19, 2017.

[7] G. Kim, J. Humble, P. Debois, and J. Willis, The DevOps Handbook : How to Create World-Class Agility, Reliability, and Security in Technology Organizations. It Revolution Press, 2016.

[8] E. Sweet, “DevOps Overview - An ISACA DevOps Series Whitepaper,” Rolling Meadows, IL USA, 2015.

[9] N. B. Ruparelia, “Software Development Lifecycle Models,” ACM SIGSOFT Softw. Eng. Notes, vol. 35, no. 3, pp. 8–13, 2010.

[10] R. Bierwolf, P. Frijns, and P. van Kemenade, “Project Management in a Dynamic Environment Balancing Stakeholders,” in 2017 IEEE Technology and Engineering Management Summit (E-TEMS), 2017, pp. 31–37.

[11] OWASP, “OWASP Top 10 - The Ten Most Critical Web Application Security Risks,” 2017.

[12] G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” J. Inf. Secur., 2013.

[13] K. Jendrian, “Sicherheit als Qualitätsmerkmal mit OpenSAMM,” Datenschutz und Datensicherheit - DuD, no. 4, pp. 270–273, 2012.

[14] P. Frijns, F. Van Leeuwen, and R. Bierwolf, “Project Management – A More Balanced Approach,” in 2017 IEEE Technology & Engineering Management Conference - TEMSCON 2017, 2017, pp. p254-258.

[15] R. Bean, “Interesting Times: Business Change In An Era Of Tech Disruption,” www.forbes.com, 2017. [Online]. Available: https://www.forbes.com/sites/ciocentral/2017/07/11/interesting-times-business-change-in-an-era-of-tech-disruption/#67978ce4334d. [Accessed: 29-Aug-2018].

[16] K. Schwaber and J. Sutherland, “The Scrum GuideTM The Definitive Guide to Scrum: The Rules of the Game,” 2017.

[17] K. Beck, M. Beedle, A. van Bennekum, A. Cockburn, W. Cunningham, M. Fowler, J. Grenning, J. Highsmith, A. Hunt, and R. Jeffries, “Manifesto for Agile Software Development,” 2001.

[18] M. Driver, V. Baker, W. Clark, T. Murphy, N. Wilson, D. Dunie, J. Herschmann, and K. Mann, “Gartner Report - Predicts 2018: Application Development,” 2017.

[19] F. Voehl, H. Harrington, C. Mignosa, R. Charron, H. J. Harrington, C. Mignosa, and R. Charron, The Lean Six Sigma Black Belt Handbook. Productivity Press, 2013.

[20] B. W. Boehm, “Software Engineering Economics,” IEEE Trans. Softw. Eng., vol. 10, no. 1, pp. 4–21, 1984.

[21] M. Dawson, D. N. Burrell, E. Rahim, and S. Brewster, “Integrating software assurance into the Software Development Life Cycle (SDLC),” J. Inf. Syst. Technol. Plan., vol. 3, no. 6, pp. 49–53, 2010.

[22] P. van Kemenade, “Beheersing en DevOps Veranderingen in de IV-voortbrengingsketen,” Vrije Universiteit, Amsterdam, 2017.
[23] T. Zijderhand, “IT Auditors: Shift Left,” Vrije Universiteit, Amsterdam, 2017.
[24] P. Debois, “Devops: A Software Revolution in the Making?,” Cut. IT J., vol. 24, no. 8, pp. 1–41, 2011.

Gooit Blockchain-Technologie de jaarrekeningcontrole overhoop?

De impact van Blockchain-technologie op het controleproces

Stef Zelen

Al meer dan 10 jaar is Stef Zelen een zeer toegewijde IT-Auditor met een Accountancy achtergrond. Als voorzitter van VUrORE is hij nauw betrokken bij de IT audit, compliance & Advisory opleiding aan de VU zowel tijdens als na zijn studie. In het jaar van afstuderen, 2017, is hij tevens toegetreden tot het bestuur van ISACA Nederland en in dit kader momenteel bezig met de oprichting van ISACA Students. Hiernaast is Stef een van de auteurs van de publicatie Agile Secure Software Lifecycle Management, welke in 2018 is uitgebracht naar aanleiding van Roadmap Digitaal veilige harden software van de Nederlandse overheid.

1 Inleiding

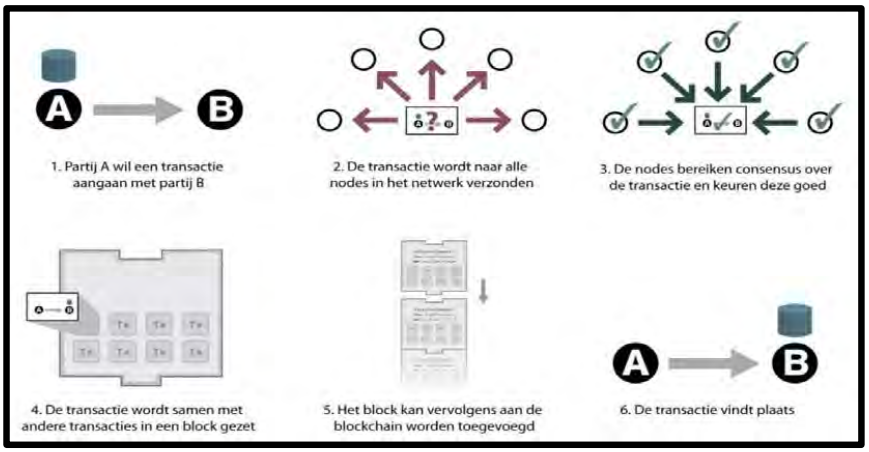
"De fysieke wereld verschuift naar de virtuele wereld"

In de laatste decennia is veel veranderd in de maatschappij. Kijk naar de impact van digitalisering, welke heeft gezorgd voor de razendsnelle opkomst van nieuwe spelers zoals Google, Facebook, Amazon, AirBnB en Uber. De fysieke wereld verschuift geleidelijk aan naar een virtuele wereld. Maar ook in deze virtuele wereld willen stakeholders zekerheid over hun financiële situatie. En, zoals van oudsher, komt dan de accountant op het toneel: de accountant is tenslotte de onafhankelijke derde, die toetst of de financiële informatie van een onderneming correct is en daaraan een redelijke mate van zekerheid verbindt. De vraag is echter of de accountant voldoende digitaal onderlegd is om, in de nabije toekomst, een oordeel te kunnen blijven vormen over de financiële situatie van de onderneming. De kwaliteitsbewuste accountant ziet ook wel dat de implementatie van de digitale trends risico's met zich meebrengen die niet langer onderbelicht kunnen blijven. En hoe moet de accountant omgaan met de komst van een technologie zoals blockchain? Deze technologie wordt gezien als de grootste technologische innovatie sinds het internet en wordt aangemerkt als disruptief.
Naar verwachting zal het ook zijn impact gaan hebben op de controlewerkzaamheden van de accountant. Sommigen stellen zelfs, dat deze technologie de accountant overbodig zal maken. Vooralsnog lijkt het meer op een technologie die het nodig acht een andere blik te gaan werpen op informatie en processen. In de basis kan het op twee verschillende manieren impact hebben op de controlewerkzaamheden van de accountant:

1 De te controleren organisatie maakt gebruik van blockchain technologie;
2 De accountant gebruikt blockchain technologie voor de uitvoering van de controle.

Dit onderzoek zal ingaan op de eerste situatie, en onderzoeken op welke wijze het controleproces van de accountant moet worden aangepast door de implementatie van blockchain technologie bij organisaties.

Wat is nu precies Blockchain?
Maar wat is nu precies blockchain? Blockchain is een databasetechnologie die voor de vastlegging en verwerking van allerlei transacties te gebruiken is; en een andere manier van organiseren mogelijk maakt (Vos, 2017). De registratie gebeurt niet in een centraal systeem maar decentraal, verspreid over vele computers van verschillende beheerders die de transacties controleren waardoor het praktisch onmogelijk is om fouten te maken of te frauderen (Roorda, Zeven vragen over blockchain, 2016). Daarbij gebruikt het technologie die stappen in processen volledig automatiseert, stappen waarvoor nu menselijke tussenkomst nodig is (Vos, 2017). Als een blockchain transactie wordt gevolgd, wordt de werking van deze technologie direct duidelijk.
Deze werkwijze maakt blockchain technologie interessant: het impliceert niet alleen een andere technologie, maar ook een andere manier van organiseren. Het vertrouwen dat een blockchain geeft, komt tot uiting in de gevormde digitale handdruk op transacties die wordt vastgelegd in een digitaal gedecentraliseerd grootboek. Iedereen die deelneemt, heeft een kopie van het grootboek op zijn computer staan. Het kan de klassieke rol van betrouwbare tussenpersoon overbodig maken (Vos, 2017).



Figuur 1: Werking Blockchain

1.1 Probleemstelling

Door toepassing van blockchain kunnen gebruikers van deze technologie tezamen een globale versie van hun waarheid onderhouden. Met deze betrouwbare gedeelde werkelijkheid ontstaat vertrouwen, zonder dat een centrale macht zoals een accountant nodig is (Bolt, 2017). Zal de accountant hierdoor in de toekomst buitenspel worden gezet? In een utopia waar het gehele financiële stelsel gebaseerd is op blockchain technologie, klopt de informatie altijd en is fraude niet meer mogelijk (Rückeshäuser, 2017). Er moet echter nog veel veranderen in de organisaties om de accountant geheel overbodig te maken, maar dat de accountant zijn huidige controleaanpak en bijbehorende werkzaamheden moet transformeren is een feit.

Het vooraf programmeerbare en open karakter van een blockchain stelt ons in staat om de wereld van accountancy compleet opnieuw uit te vinden, op te bouwen en te innoveren. Blockchain zal alles efficiënter en transparanter maken, en met heel veel minder bureaucratie, control- en verantwoordingssystemen. Idealiter zijn er bijna geen menselijke handelingen meer nodig voor de transactieverwerking en is de planning en control cyclus met al zijn vermoeiende rapportages en formats overbodig (Voskuilen, 2017).

Een goedkeurende accountantsverklaring, om vast te stellen of wel een getrouw financieel beeld van de onderneming gegeven wordt, is dan niet meer nodig. Immers, de goedkeuring is toch vooraf gegeven voordat de transacties de blockchain in gaan, alle accountancy- en verantwoordingsregels zijn tenslotte vooraf geprogrammeerd en verwerkt in de blockchain(Voskuilen, 2017). De vraag hierbij is of het object van de controle gaat veranderen, of dat slechts de wijze van controleren anders wordt.

1.2 Doelstelling en Centrale vraag

Het doel van dit onderzoek is om inzicht te verschaffen in de veranderingen in de Nederlandse controlepraktijk wanneer organisaties gebruik gaan maken van blockchain technologie. Hierbij zal specifiek gekeken worden hoe de controlewerkzaamheden van de accountant zullen veranderen door de implementatie hiervan in de financiële en operationele processen van de controleplichtige organisatie. De hierboven geschetste situatie heeft geleid tot de centrale onderzoeksvraag:

Op welke wijze wordt het controleproces van de accountant beïnvloed door de implementatie van blockchain technologie bij organisaties?

En de daarbij behorende volgende deelvragen:

1 Wat is de huidige stand van zaken met betrekking tot accountantscontrole in relatie tot blockchain technologie?

2 Welke risico's en beheersingsmaatregelen komen voort uit blockchain technologie?
3 Kan het huidige controleproces van de accountant gebruikt worden voor de controle van organisaties die gebruikmaken van blockchain technologie?

2 Blauwdruk van blockchain

2.1 Definitie van blockchain

Blockchain wordt gezien als een vorm van databeheer, die het beste kan worden vergeleken met een spreadsheet of een Excel werkblad. Het universele grootboek van de blockchain is niets anders dan een lijst zoals in een spreadsheet. Welke is gedeeld met iedereen ter wereld, waarbij iedere gebruiker van de keten een exacte kopie van die lijst krijgt en kan zien wat er in staat. En wijzigingen in de spreadsheet worden direct overgenomen op alle andere kopietjes van de lijst. Het resultaat is, dat iedereen altijd naar dezelfde lijst met gegevens kijkt, overal ter wereld, op elk moment (Bolt, Wat is blockchain, 2015). Maar deze vergelijking van blockchain met een Excel spreadsheet levert nog geen bruikbare definitie op. In dit onderzoek wordt de volgende definitie gehanteerd:

Blockchain is een tijd vaste, onbetwistbare gedistribueerde database die alle transacties binnen het systeem op chronologische wijze heeft vastgelegd van het begin af aan. Iedere transactie binnen het blockchain network bezit een eigen lokale kopie van de hele database en omdat de nodes door middel van algoritmen consensus bereiken blijven alle kopieën synchroon en is er geen centrale autoriteit nodig.

2.2 Dimensies binnen Blockchain

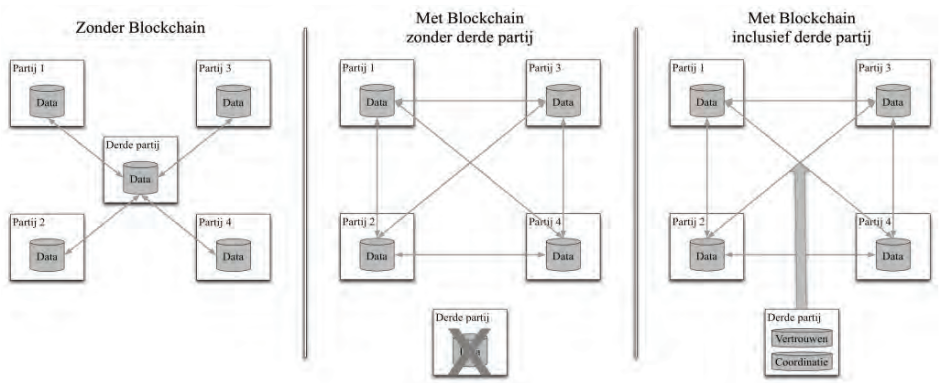
Als we puur naar het begrip blockchain kijken, dan kunnen we drie lagen onderkennen: De technologische blockchain laag; protocol laag en de applicatielaag. De eerste laag betreft de onderliggende technologie, genaamd blockchain. Blockchain technologie is een combinatie van verschillende technologieën, waardoor het een uniek voorbeeld van 'fusion of technologies' is (Schwab van, 2016). De tweede laag die te onderkennen valt is die van dataopslag, ofwel de laag waar de vraag van waar en hoe transacties worden opgeslagen en verwerkt aan bod komt. De laatste laag betreft die van de applicatie zelf, waar de blockchain feitelijk voor wordt gebruikt.

Figuur 2: De lagen binnen Blockchain

2.3 De werking van een blockchain

Blockchain kan volgens Schwab als volgt worden gezien: "*radically new approach that revolutionize the way in which individuals and institutions engage and collaborate"* (Schwab van, 2016)**.** De werking van deze nieuwe technologie wordt hieronder uiteengezet.
Blockchain technologie zorgt ervoor dat alle aangesloten computers op het blockchain netwerk, ofwel de nodes, worden voorzien van de transactiedata (Vigna, 2015). Deze data wordt continu geregistreerd en

vastgelegd in bestanden genaamd blokken[5]. De blokken zijn binnen het netwerk op een chronologische volgorde gerangschikt, waarbij de nieuwe transacties worden toegevoegd aan het uiteinde van de keten. Deze eigenschap maakt blockchain technologie zo uniek (Bolt, 2015). Een keten bestaat uit twee onderdelen: een blokhoofd en een inhoud (wikipedia, 2017). In de blokken staan de eigenlijke bij te houden data en de blokhoofden bevestigen wanneer en in welke volgorde blokken geregistreerd zijn (tijdstempels om dubbele uitgaven en conflicten te vermijden). In het blokhoofd is ook een verwijzing naar het vorige blok verwerkt (wikipedia, 2017).
Deze blokken ofwel de transactiedata staan direct ter beschikking van het netwerk en kunnen niet veranderd of verwijderd worden nadat ze zijn toegevoegd aan de keten. Doordat er gebruik wordt gemaakt van een privaat-publieke sleutel encryptie is het niet te traceren welke individu de publieke transactie uitvoert (Kelly, 2015). De cryptografische sleutels worden niet gedeeld met andere gebruikers waardoor enkel de eigenaren toegang hiertoe hebben. Een blockchain maakt binnen het netwerk gebruik van 'nodes' om consensus te bereiken over de geldigheid van elke transactie. Deze validatie methode is gebaseerd op een vergelijking tussen de historische gegevens in de keten en de huidige transactie (Vigna, 2015). Nadat er overeenstemming is bereikt kan de transactie worden opgenomen in het gedistribueerde grootboek en wordt de blockchain bijgewerkt (Van de Velde, 2016). Blockchain technologie maakt decentrale besluitvorming dus mogelijk. Dit wil zeggen dat er geen centrale controlerende partij meer nodig is voor het goedkeuren van transacties (Bruin de, 2016). Plat gezegd: de rol van de notaris, bank, accountant of gemeentelijke registratie wordt overgenomen door software. Daarom wordt blockchain gezien als een technologie die een grote impact zal hebben op de economie. Onder aan de streep is de blockchain een databasetechnologie. Welke voor allerlei transacties gebruikt kan worden (Bolt, 2015).



Figuur 3: Rol van de derde partij in een blockchain

3 Blockchain technologie en de accountant

Al zeker 10 jaar heeft de accountancybranche te maken met automatisering, digitalisering en standaardisering. De inzet van ICT heeft bij de grotere kantoren de productiviteit, in termen van omzet per FTE, opgeschroefd (ING, 2015). Integriteit, objectiviteit, deskundigheid, geheimhouding, zorgvuldigheid en professioneel gedrag zijn essentiële waarden voor iedere accountant. Een auditor geeft zekerheid aan bestuur en management van een organisatie over de mate waarin de bedrijfsvoering wordt beheerst en over de toereikendheid van de risicobeheersingssystemen, inclusief de daarbij behorende rapportages.

[5] Blokken kun je zien als afzonderlijke pagina's van een grootboek (avexo, 2017)

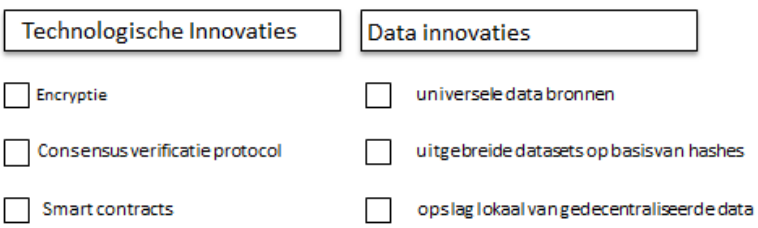
Waar het voeren van een boekhouding in het verleden voornamelijk handmatig gebeurde; zien we dat dit heden ten dage geheel digitaal gaat op basis van gespecialiseerde boekhoudprogramma's. En in de toekomst met de komst van blockchain technologie, wordt het zelfs mogelijk de oude gedachte van dubbel boekhouden deels los te laten. We hoeven bijvoorbeeld niet langer een centrale boekhouding te voeren, het vertrekpunt is immers een gedeelde bron van de waarheid (een gedeelde database). Dat biedt kans voor een enorme efficiëntieslag, de kosten voor beheer en gebruik van applicaties kunnen structureel omlaag. Hiernaast wordt het vertrouwen gedigitaliseerd met de komst van de blockchain. Immers, in de blockchain is vertrouwen een 0 of een 1. Het digitaliseren van vertrouwen gebeurt gedistribueerd en wordt verwerkt in de processen, in de vorm van smart contracts (Zuidam, 2016). In een (geautomatiseerd) proces kan worden ingebouwd dat een bepaald document X vertrouwen nodig heeft, om een specifieke actie in gang te zetten. Op deze manier kunnen geldstromen geautomatiseerd en voorwaardelijk worden geïmplementeerd. Uiteindelijk zal blockchain onder de motorkap verdwijnen. Waardoor het een integraal onderdeel wordt van allerlei dagelijkse financiële transacties in de boekhouding. Het gebruik van de blockchain zal net zo vanzelfsprekend als online bankieren, WhatsApp en email worden (morgen, 2017).

3.1 De beloftes en risico analyse van Blockchain technologie

3.1.1 De beloftes van blockchain technologie

Blockchain technologie is ontstaan vanuit een aantal technische concepten uit het verleden, die zijn gecombineerd en op deze wijze hebben gezorgd voor een aantal nieuwe innovaties op het gebied van technologie en data-efficiëntie. De digicommissaris Bas Eenhoorn zegt dat de eigenschappen van blockchain passen als een handschoen op de informatiesamenleving van de toekomst (Pomp & Hartog , 2017). Blockchain technologie bevat nieuwe methodes en toepassingen van encryptie technologieën, die beveiliging en anonimiteit van gevoelige gegevens mogelijk maakt zelf in gedecentraliseerde publieke netwerken zoals het Bitcoin netwerk (Van de Velde, 2016).

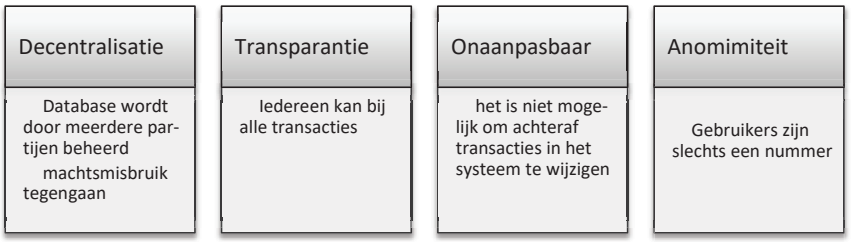
Het protocol van wederzijdse consensus verificatie, welke blockchain gebruikt, is een van de andere innovaties. Dit protocol garandeert dat de algemene data correct blijft en het staat het netwerk toe onderling te beslissen zonder dat daar een centrale autoriteit voor nodig is. Een derde innovatie betreft de smart contracts, dat is programmacode geüpload in het grootboek in plaats van platte data invoer (Van de Velde, 2016). Smart contracts zijn een manier om de rechten en verplichtingen van de gebruiker om te zetten in digitale informatie. Deze contracten kunnen wel is de innovatie zijn, die voor de echte verandering gaat zorgen in de accountancybranche, gezien het een aantal taken kan uitvoeren die momenteel worden uitgevoerd de accountant (Pinna, 2016).



Figuur 4: Innovaties van blockchain technologie

Bovengenoemde innovaties betreffen technologische innovaties, de basis waarop blockchain is opgebouwd. Hiernaast zijn er ook een aantal innovaties op gebied van dataverwerking te onderkennen, waardoor er efficiënter met data kan worden omgegaan (Lundstrom, 2016). De huidige gefragmenteerde data

structuren en methodes voor het opslaan en overeenstemming bereiken over de inhoud van de datasets is een complex proces en heeft te maken met een tekortkoming aan standaardisatie. Het gevolg hiervan is, dat een ieder zijn eigen database er op na houdt en in zeer omvangrijke systemen is dit zeer inefficiënt en brengt hoge kosten met zich mee. Vanuit het perspectief van de accountant zien we dat elk te controleren organisatie boekhoudsoftware (bij grotere organisaties een ERP oplossing) kiest welke het beste bij hun organisatie past, waarbij de administratieve inrichting specifiek wordt afgestemd op de desbetreffende organisatie. Door blockchain zou je dit kunnen uniformeren en binnen het netwerk zou iedereen gebruik kunnen maken van dezelfde administratieve inrichting, denk hierbij aan een uniform rekeningschema (Van de Velde, 2016). Van de Velde, (2016), stelt verder dat blockchain het gebruik van gegevens efficiënter kan maken, door middel van de verschillende gebruikers gebruik te laten maken van de universele data die is opgenomen in desbetreffende blockchain applicatie en waardoor deze voor alle gebruikers direct beschikbaar is. Door nieuwe encryptie methodes is het mogelijk geworden verschillende soorten data op te nemen in het gedecentraliseerde grootboek, waardoor de omvang van datasets enorm zal toenemen (Van de Velde, 2016). De laatste innovatie op het gebied van de data, is het feit dat de data bij de gebruiker lokaal is opgenomen waardoor het efficiënter te raadplegen is. De toepassing hiervan neemt eigenlijk het belang van grote centrale databases af en hiernaast ook de noodzaak om de datasets tussen gebruikers af te stemmen, want deze is al door blockchain technologie gesynchroniseerd. Het voorkomt ook dataverlies doordat alle gebruikers de data lokaal beschikbaar hebben (Van de Velde, 2016).
De beschreven innovaties zijn te vertalen naar een aantal voordelen van blockchain technologie, echter gezien de status van blockchain wordt er niet gesproken over voordelen maar van beloftes. De volgende beloftes op het gebied van blockchain technologie worden onderkend: Decentralisatie, transparantie, onaantastbaar en anonimiteit.



Figuur 5: De beloftes van Blockchain

Decentralisatie
In een publieke blockchain, ofwel een volledig gedecentraliseerde configuratie hebben alle gebruikers alle rechten. Bitcoin is een goed voorbeeld van een publiekelijk toegankelijke, gedecentraliseerde blockchain en is bijzonder betrouwbaar gebleken. Wanneer een meerderheid van de benodigde rekenkracht om consensus te bereiken in handen is van partijen met goede intenties, is het onwaarschijnlijk dat de data in een blockchain kan worden gemanipuleerd (EY, 2017).

Transparantie
Met behulp van het gecentraliseerde grootboek kun je altijd het laatste saldo berekenen. De informatie over de transacties is openbaar, echter de adressen van de transacties betreffen anonieme codes zodat de betrokken partijen anoniem zijn. In de traditionele financiële systemen is er altijd een centrale instantie die de inkomende en uitgaande transacties toetst, overboekingen verwerkt, het saldo controleert en de transactiedata centraal opslaat. Bij de blockchain is er sprake van een decentrale databank met transactiegegevens op alle computers die deelnemen aan de desbetreffende blockchain. Daarmee heeft elke gebruiker van de blockchain toegang tot de complete set van transacties, die daarmee van niemand eigendom en dus openbaar is (Bader & Thorsten, 2017).

Onaanpasbaar
De onaanpasbaarheid wordt mogelijk gemaakt door het ontwerp van het systeem. Allereerst worden telkens een X aantal transacties (een blok) bij elkaar opgeteld. Hieruit wordt een controle getal berekend. Dit controlegetal wordt het eerste getal in een nieuw blok van transacties. Als je een getal in een oud block probeert aan te passen, dan werkt dit door op alle volgende blokken. Alle transacties worden door alle computers gecontroleerd. Dus als je een aanpassing maakt in jouw kopie van de blockchain, dan zullen de andere computers nalopen of alles nog wel klopt (Schep, 2017).

Anonimiteit
"Allereerst: blockchain-technologie kan worden gebruikt voor allerlei soorten systemen, ook voor systemen waarin anonimiteit niet belangrijk is. Waar anonimiteit wel benodigd is, is het wel degelijk mogelijk om perfecte controle van alle transacties te behouden zonder anonimiteit op te geven. Dit vergt enkel wat technische stappen (Roorda, 2016). De kern draait hierbij om de sleutels in de keten. Voordat een blok gebouwd en in de blockchain wordt opgenomen, moeten persoonlijke en openbare sleutels gecreëerd worden. Uit de openbare sleutel wordt een 34-cijferige reeks gebouwd, die vervolgens als blockchain adres voor de latere transacties fungeert. Hierbij is het niet mogelijk om de openbare sleutel te herleiden uit het openbare adres, waardoor de anonimiteit wordt gegarandeerd (Bader & Thorsten, 2017).

3.1.2 Risico analyse
Naast de kansen die blockchain met zich meebrengt als nieuwe technologie, zitten aan deze technologie ook een aantal nieuwe risico´s, waar maatregelen tegen getroffen moeten worden. Vanuit het oogpunt van een controlerend accountant zal hieronder gekeken worden naar de risico´s die voortkomen uit de toepassing van blockchain technologie bij organisaties. De onderkende risico´s door de accountant kunnen worden gegroepeerd in een drietal categorieën: Data gerelateerde risico's; Beveiligings, privacy en compliance risico's; Gedrags en kennis risico's.

Data gerelateerde risico's
De 51% aanval, waarmee het mogelijk wordt om de data in de blockchain te muteren, is een risico waarmee rekening gehouden dient te worden. Zeker in het geval gekozen wordt voor een private blockchain, maar met hetzelfde consensus mechanisme als bij een publieke blockchain, waar de keten enkel bestaat uit enkele gebruikers, dan is het al snel mogelijk 51% van de gebruikers te overtuigen van wat jij zegt de waarheid is en gezien er sprake is van het consensusmodel, zal dit dan worden aangenomen als de waarheid. Er zal dus goed nagedacht moeten worden over de omvang van het aantal gebruikers in de keten, want hoe groter de keten is hoe lager de kans is op een 51% attack.

Beveiligings, privacy en compliance risico's
Systeem hack, zoals eerder aangegeven is het moeilijk om de data in de blockchain te hacken, maar dit is niet het geval voor het systeem en de code op basis waarvan de blockchain applicatie is geïmplementeerd. Een bekend voorbeeld hiervan is de hack op de MTGox, een Bitcoin beurs. Deze is in 2014 gehacked en toen is er aan 700 miljoen dollars aan Bitcoin gestolen en verleden jaar (2017) is er nog een DAO incident geweest waarbij rond zestig miljoen dollar is ontvreemd.
Een ander risico is het verlies van de identiteit, door identiteitsdiefstal. Ook al wordt blockchain technologie als zeer veilig gezien en data versleuteld is, op het moment dat persoonlijke sleutel wordt gestolen om toegang te krijgen tot de blockchain, is er geen derde partij die ervoor kan zorgen dat de sleutel weer terugkomt bij de rechtmatige eigenaar. Het grootste probleem bij een dergelijke diefstal is dat er niet terug te herleiden valt welk eigendom is gestolen, gezien de anonimiteit van de blockchain. Het probleem wat zich voor zal doen voor de accountant is, dat hij een onderbouwing zoekt voor het bestaan en eigendom, echter door de diefstal is dit niet mogelijk. Dit zal leiden tot onjuiste conclusies tijdens de controle, gezien

hij niet kan vaststellen wat er is gestolen. Een ander risico is dat de toegepaste cryptografie mogelijk in de toekomst toch uitgelezen kan worden met bijvoorbeeld de komst van quantum computing, dit zou de blockchain technologie kunnen ondermijnen.

Gedrags en kennis risico's

Het gevaar is dat organisaties blockchains oplossingen gaan implementeren zonder dat ze de techniek erachter begrijpen. Doordat ze kennis over blockchain technologie niet goed beheersen nemen ze beslissingen die mogelijk niet de juiste zijn. Het is daarom van belang afdoende kennis op te doen van de materie alvorens blockchain applicaties te implementeren. Dit speelt ook een belangrijke rol voor de accountant hij moet onderkennen dat hij mogelijk niet de juiste kennis in huis heeft om de organisatie, die gebruik maakt van blockchain applicaties, zelfstandig te kunnen controleren.

3.2 Veronderstelde impact op het controleproces

Over het algemeen zit het onderzoek naar de toepassing van blockchain technologie nog in de experimentele fase, met uitzondering van een aantal onderzoeken die de fase van operationalisering hebben bereikt. Binnen de accountancy branche valt op dat er sprake is van een tweedeling, waarbij de BIG 4 investeert in de blockchain en de overige accountancykantoren blockchain nog even links laten liggen[6].

Op basis van de huidige controlewerkzaamheden en in vergelijking hoe het controle object zich heeft ontwikkeld en zich technologisch steeds verder aan het doorontwikkelen is, is de vraag of de huidige accountant nog wel de benodigde kennis bezit om een jaarrekening anno 2017 zelfstandig te controleren. Als we vervolgens kijken naar blockchain technologie en hoe deze aan het ontwikkelen is in de praktijk in zowel de publieke als private sector, kunnen we ons afvragen of accountant momenteel geen digibeet is en in de toekomst zich zal moeten omscholen en tenminste ook de technische vaardigheden van een IT-auditor moet bezitten om zijn beroep te kunnen blijven uitoefenen.

De rol van de accountant zal gaan veranderen, echter hoe is afhankelijk van de wijze waarop blockchain geïmplementeerd zal gaan worden bij organisaties. De verwachting is dat accountant meer zal gaan steunen op de werking van de smart contracts en daardoor zijn focus zal verleggen naar de bedrijfsprocessen van de te controleren organisatie.

Door blockchain wordt het mogelijk het object van onderzoek aan te passen, en niet langer enkel te steunen op de jaarrekening. De jaarrekening is slechts een momentopname in tegenstelling tot de mogelijkheden van de controle op een smart contract binnen een blockchain. De smart contracts zijn namelijk het startpunt van de blockchain en op basis waarvan transacties door de keten worden geleid. De accountant zal wel moeten blijven toezien op het toetsen van de opzet, bestaan en werking van administratie organisatie en de interne beheersing van de organisatie. Op moment dat de administratieve organisatie niet op de juiste wijze is ingericht is het mogelijk dat de daarop afgestemde blockchain niet juist functioneert of bepaalde risico's niet afdekt. Door het object van onderzoek te wijzigen in de smart contracts, is het mogelijk het controleproces niet achteraf maar vooraf te laten plaatsvinden. Hierdoor wordt het ook mogelijk continuous auditing toe te gaan passen.

Een andere kans voor de accountant zou kunnen zijn, dat de accountant een onderdeel van de blockchain gaat worden, als bijvoorbeeld een keynode binnen de keten van een blockchain, echter hierdoor stap je wel direct af van de publieke blockchain technologie en kom je terecht in een private blockchain en de vraag is of dit gewenst is.

Een derde kans voor de accountant is om de gehele blockchain applicatie te controleren op het moment dat deze wordt gebouwd. Zie het als certificering van software alvorens het in gebruik kan worden genomen, dit zit tegen de controlewerkzaamheden op de smart contracts aan. Echter de vraag is of de huidige

[6] Met enkele uitzonderingen hierop daargelaten.

en toekomstige accountant afdoende kennis heeft om deze controle uit te voeren, en of hij zich in de toekomst zou moeten bijscholen of dat er juist gesteund moet worden op een externe deskundige (blockchain auditor).
Het bijscholen van de huidige accountant is pas nodig als de blockchain applicaties operationeel worden in organisaties. Hiernaast is momenteel nog weinig wetgeving aanwezig op dit vlak en mogelijk kunnen bepaalde blockchain applicaties niet worden geïmplementeerd omdat de onderneming dan niet zou voldoen aan de wettelijke verplichtingen. Doordat de wetgeving en zeker ook de beroepsorganisaties van de accountants maar beperkt bezig zijn met de effecten van blockchain technologie; En ook niet bezig zijn de wet en regelgeving hierop aan te passen, zal de operationalisering van de blockchain worden geremd.
Zoals eerder gesteld is het de vraag of de accountant wel de aangewezen persoon is om de controle van een blockchain op zich te nemen. Als we kijken naar het controleren van de smart contracts zou je zeggen dat dit prima past in het takenpakket van de accountant, zeker als een uitspraak moet worden gedaan over de juistheid en volledigheid van een smart contract binnen een blockchain. Hiernaast is de gedachte dat de accountant de gehele blockchain zou kunnen gaan controleren. Echter de gemiddelde accountant zal niet direct de kennis hebben om een blockchain te controleren. De controle van smart contract van een blockchain is misschien al een te grote uitdaging voor de accountant. Hij zou hierop wel kunnen inspelen, door zijn vaardigheden hierop aan te passen. Ook wordt gesproken over het feit dat de accountant onderdeel moet gaan uitmaken van de keten als een vertrouwde gebruiker. De vraag is wat de meerwaarde is om een accountant toe te voegen aan de keten, welke extra zekerheid geeft hij en op welke wijze zou hij dit kunnen doen.

De Nederlandse bank kwam met de conclusie: Als blockchain het ántwoord is… wat is dan de vraag?

De mogelijkheid bestaat dus dat de kerntaken van de accountant zullen wijzigen in het controleproces, zeker als de transactie gerelateerde en gegevensgerichte werkzaamheden naar de achtergrond verschuiven tijdens een controle. En dit wordt veroorzaakt doordat het door blockchain technologie mogelijk is geworden transacties onafhankelijk te valideren, waar in het verleden de accountant vaak de rol op zich nam van validatie. De rol van de accountant zou kunnen verschuiven in de waardeketen (value chain), naar een governance rol rondom het gebruik van verschillende type blockchains. (Nick Martindale citaat: Alex, 2016). Andrew Wingfield[7] verwacht dat dit mogelijk kan leiden tot de ontwikkeling van real-time controles ofwel continuous auditing. “one of the most compelling use-cases for blockchains is their ability to provide a live, indelible record of financial transactions, suchs as derivates trades, which could give accountants the ability to perform, in effect, real-time, ‘smart’ audits of the capital and risk positions of banks and other financial services clients, “hij zegt” It’s likely that, on the other hand, in the medium-to-long-term, blockchain-driven solutions could reduce the need for many lower quantum, high-volume manual audit processes”. (Nick Martindale citaat: Alex, 2016)

“I don’t think it is going to cut our profession out,”
L. Gary Boomer, CPA/CITP, CGMA, former CEO of Boomer Consulting (CGMA, 2017),

Volgens Rube Goldberg is het van belang dat de accountant is goed gaat kijken naar zijn controleaanpak en het weglaten van werkzaamheden die geen toegevoegde waarde leveren. De focus moet liggen op de controleaanpak die in de toekomst wel waarde aan het controleproces kan toevoegen (CGMA, 2017).
Bij de controle van een jaarrekening geeft een ‘time stamping’[8] zekerheid, maar dat zegt nog niets over de kwaliteit van de onderliggende data. Daarvoor geldt nog steeds garbage in garbage out. Je kunt wel iets zeggen over de oorspronkelijke datum en tijd waarop documenten zijn vastgesteld, maar je zal steeds een

[7] Corporate partner at King & Wood Mallesons

[8] vaststellen dat een transactie op een specifiek moment plaatsvond en in de blockchain is vastgelegd.

controle moeten uitvoeren op de achterliggende data. Door de intrede van blockchain zal je meer naar begin van het transacties verwerkingsproces moeten gaan kijken. Maar het is te eenvoudig om te stellen, dat door blockchain technologie de onafhankelijke derde als vastlegger en bewaarder van de gemaakte afspraken overbodig zou worden. Het antwoord hierop kan pas worden gegeven in een wereld van blockchain. De verwachting is dat grote technologische bedrijven als eerste de blockchain technologie in sub processen zullen gaan implementeren, en als consequentie hiervan zullen de grote accountantskantoren in een versneld tempo kennis tot zich nemen om deze organisatie te kunnen blijven controleren (Alles, 2015).

3.3 Analyse

Op basis van het literatuuronderzoek is gesteld dat de huidige accountant niet voldoet aan de benodigde vereisten om een jaarrekening anno 2017 te controleren. Op basis van de bevindingen vanuit de interviews wordt deze stelling niet bevestigd De geïnterviewde accountants geven aan dat de accountant de eindverantwoordelijke is en zal blijven. Hij is verantwoordelijk voor kwaliteit van de geleverde prestatie en hierbij kan hij ook externe deskundigen inschakelen om de kwaliteit te waarborgen. Deze externe deskundigen kunnen namelijk de (technische) tekortkomingen van de accountant ondervangen in de uitvoering van de controleopdracht.

Moet de accountant dan misschien in de toekomst een mix zijn van de traditionele accountant en de IT-Auditor? De vaardigheden van de accountant zullen afhankelijk moeten zijn van het object van onderzoek en de rol die de accountant hierin mogelijk zal gaan vervullen. Vooruitkijkend zijn de volgende rollen voor een accountant in een wereld van blockchain mogelijk:

- controleur van de smart contracts;
- strategische adviseur van de onderneming bij de inrichting van de blockchain;
- een van de key nodes in een blockchain netwerk;
- Assurance afgeven bij een blockchain implementatie.

Als we tenslotte kijken naar de impact van blockchain technologie op de controlepraktijk, zien we een aantal kansen voor de accountant op het moment dat er blockchain oplossingen bij de ondernemingen worden geïntroduceerd. Het controle proces zal door de aanwezigheid van blockchain technologie zeker gaan wijzigen en het zal de huidige jaarrekeningcontrole overhoop halen. Het is zelfs geen vreemde gedachte dat het object van onderzoek zal wijzigen bij de aanwezigheid van een of meerdere blockchains bij de controleplichtige organisaties. Waar in de traditionele situatie de jaarrekening het object van onderzoek is, en waarbij de juistheid en volledigheid van de financiële administratie wordt getoetst. Is dit in de wereld van blockchain niet langer nodig, omdat de cijfers van de financiële administratie altijd juist en volledig zijn op het moment dat het transactieproces is verwerkt met behulp van een blockchain. De specialisten geven aan dat niet langer de jaarrekening (financiële administratie) het object van onderzoek zou moeten zijn maar de opgestelde smart contracts. Indien de controle zich zal gaan focussen op de smart contracts, dan verschuift het controleproces van de eindejaarswerkzaamheden op de standen en stromen van de financiele administratie naar de inrichting en ingebruikname van smart contracts en de blockchain in het algemeen.

4 Conclusies en aanbevelingen

De accountant brengt met zijn controleverklaring vertrouwen voor alle belanghebbenden. De term “belanghebbende partijen” betreft een breed spectrum aan partijen, welke onder andere de volgende partijen omvatten: aandeelhouders, banken, belastingdienst, raad van bestuur, toezichthouders, leveranciers, milieuorganisaties en enzovoort. Veel van deze mensen ontbreekt de technische kennis, om blindelings te steunen op innovaties in de technologie; en het huidige speelveld aan risico’s op zowel operationeel als juridisch vlak te overzien. Dit maakt blind vertrouwen, een onacceptabel risico. Er zal dus altijd een onaf-

hankelijke functionaris noodzakelijk zijn om zekerheid ofwel vertrouwen te geven, aan alle belanghebbenden, over elk operationeel proces. Nu we hebben geconcludeerd dat de rol van de accountant niet verdwijnt, omdat het maatschappelijk verkeer vraagt om vertrouwen. Is het nog wel de vraag op welke wijze het controleproces van de accountant beïnvloed wordt, door de implementatie van blockchain technologie bij organisaties.

Op het moment dat blockchain technologie wordt geïmplementeerd, zal het controleproces zo en zo gaan veranderen, gezien de risico's en interne beheersingsmaatregelen verbonden aan blockchain anders zijn dan zonder gebruikmaking van deze technologie. De wijze waarop het controleproces gaat wijzigen is afhankelijk van hoe de blockchain in de financiële administratie bij een organisatie er uit komt te zien en of het object van onderzoek van de accountant gaat wijzigen door de implementatie van blockchain bij organisaties. Op basis van de literatuurstudie en de expert interviews zijn een aantal scenario's denkbaar. Bij alle scenario's wordt uitgegaan van een private blockchain, het voordeel van een private blockchain ten opzichte van een publieke blockchain is dat er minder technische barrières aanwezig zijn om de blockchain operationeel te krijgen en daarnaast is de functionaliteit van een private blockchain breder.

We concluderen dat er verschillende scenario's realistisch zijn met betrekking tot mogelijke wijzigingen in het controleproces van de accountant. De volgende vier scenario's worden onderkend:

1 De accountant gaat de smart contracts controleren;
2 De accountant steunt op de werkzaamheden van de blockchain auditor;
3 De accountant gaat data elementen controleren;
4 De accountant wordt een onderdeel van de blockchain keten.

Hieronder worden de geschetste scenario's toegelicht, waarbij achtereenvolgens wordt ingegaan op het type blockchain, het object van het onderzoek en de wijze waarop het controleproces van de accountant wordt beïnvloed.

De accountant gaat de smart contracts controleren

Zoals gezegd is er sprake van een private blockchain waarbij de keten uit tenminste zeven gebruikers bestaat. Welke type consensus er binnen de keten wordt gebruikt is niet zozeer van belang. Uiteraard zijn elementen van triple entry accounting aanwezig en staan de smart contracts van blockchain centraal.

Het object van onderzoek voor de accountant zal niet wijzigen, het betreft nog altijd de jaarrekening, maar door de aanwezigheid van een of meerdere blockchain applicaties binnen een te controleren organisatie zal het controleproces wijzigen. De fases van het controleproces blijven gehandhaafd maar het zwaartepunt van de controlewerkzaamheden zal verschuiven. De standen en stromen van de posten van de jaarrekening per jaareinde die pas na het einde van het boekjaar kunnen worden gecontroleerd hoeven niet langer leidend te zijn. Doordat de financiële transacties in een blockchain applicatie worden verwerkt is er al zekerheid over dit proces. Echter dit betekent niet direct dat de accountant in zijn geheel overbodig is geworden, want aan de invoerzijde is nog altijd de vraag of de informatie op de juiste wijze wordt ingevoerd en hiernaast moet een blockchain applicatie wel op de juiste wijze worden ingericht om te kunnen vaststellen dat het transactie verwerkingsproces werkelijk plaatsvindt in de keten van de blockchain applicatie. Betreffende de risico's verbonden aan de invoer van data is niets gewijzigd ten opzichte van de situatie zonder blockchain, de risico's zullen voornamelijk worden afgedekt door de interne beheersingsmaatregelen van de organisatie. De accountant zal dus zoals van oudsher een interim controle moeten blijven uitvoeren waarbij de elementen opzet, bestaan en werking van de administratieve processen wordt getoetst. Het is hierbij wel mogelijk dat bepaalde processen worden verkort door de inzet van blockchain technologie. Kijkend naar deze techniek zal het nodig zijn de smart contract die ten grondslag liggen aan een blockchain te gaan controleren. Om dit mogelijk te maken zal de accountant moeten beschikken over vaardigheden die momenteel nog niet op zijn palet van vaardigheden aanwezig zijn. Uit zowel de literatuur als de interviews blijkt dat de accountant onvoldoende kennis heeft op het gebied van de technische informatietechnologie. De smart contracts zijn geprogrammeerd dus de accountant zal kennis moet hebben van de betreffende programmeertaal om de inhoud van deze contracten te kunnen controleren. Waarna de gegevensgerichte werkzaamheden op de balansposten achterwege kunnen blijven. Hiernaast is sampling niet

langer nodig omdat de transactieverwerking goed of geheel fout gaat, gezien het gehele verwerkingsproces afhankelijk wordt van de blockchain applicatie.

De accountant steunt op de werkzaamheden van de blockchain auditor
Qua opbouw van blockchain is dit tweede scenario gelijk aan het eerste scenario en ook het object van onderzoek is nog altijd de jaarrekening. In dit scenario wordt onderkend dat de accountant niet de kennis en vaardigheden heeft om een oordeel uit te kunnen spreken over de blockchain applicatie en de daarin opgenomen smart contracts. Er wordt zelfs gesteld dat dit ook te specialistisch zal zijn voor de gemiddelde IT-auditor, laat staan voor de huidige opgeleide accountant. Voor de controle van de blockchain en smart contracts zal waarschijnlijk een nieuwe functie ontstaan. (de blockchain auditor). Deze specialist zal zekerheid verlenen aan blockchain applicaties en de daarbij van toepassing zijnde smart contracts. Deze zekerheid kan tot uitdrukking komen met behulp van een specifieke controleverklaring, zoals een 3402-verklaring, SOC1, SOC2 of een ISO certificering. De blockchain auditor moet je vergelijken met de specialistische auditors die zich bezighouden met het afgegeven van verklaringen voor service organisaties. De accountant zal dus gaan steunen op deze verklaring, die een uitspraak doet over de gecontroleerde blockchain. Het controleproces zal beperkt wijzigen doordat de controle op de blockchain applicatie wordt uitbesteed. Indien de accountant kan concluderen dat hij kan steunen op de blockchain, dan is het mogelijk om een groot aantal gegevensgerichte werkzaamheden achterwege te laten, doordat deze werkzaamheden reeds gecontroleerd zijn door de blockchain auditor, die specifiek naar het verwerkingsproces van een blockchain heeft gekeken.

De accountant gaat data elementen controleren
Het object van de controle zal gaan veranderen, de accountant zal niet langer zekerheid verlenen bij de jaarrekening omdat hier niet langer toegevoegde waarde aan verbonden zit, door de introductie van blockchain applicaties. Blockchain zal in verschillende vormen geïmplementeerd worden binnen de te controleren organisaties, waardoor het mogelijk is om data te controleren aan het begin van het verwerkingsproces. Hierdoor ligt continuous auditing in handbereik. Hierbij moeten we wel opmerken dat ook blockchain applicaties zelf gecontroleerd moet worden alvorens op deze applicaties gesteund kan worden, de vraag is of de accountant of een externe specialist deze controle op zich neemt.

De accountant wordt een onderdeel van de blockchain keten.
Het laatste scenario is een scenario welke niet door alle experts als haalbaar wordt gezien, maar zeker in de beginperiode van de implementatie zou het toch een optie kunnen zijn. Het laatste scenario is dat de accountant een geheel andere rol gaat vervullen. Doordat de accountant van oudsher wordt gezien als vertrouwenspersoon, kan hij als keynode gaan optreden in de blockchain keten. Zeker in de begindagen dat organisaties blockchain willen gaan implementeren, zal er twijfel bestaan over het vertrouwen dat ze kunnen hebben in de blockchain. Door de accountant als vertrouwenspersoon toe te voegen in de keten als node, is het mogelijk dat de overige partijen de betreffende blockchain eerder zullen gaan accepteren. Dit kan zelfs worden gestimuleerd door het consensusmodel aan te passen, in een consensusmodel waarin de accountant als node een veto kan uitspreken. Echter op moment dat een accountant betrokken wordt in een blockchain als een node, dan is het niet langer mogelijk om ook controlewerkzaamheden voor deze cliënt uit te voeren, je kunt deze rol namelijk zien als advieswerkzaamheden waardoor hij zijn onafhankelijke positie niet langer kan waarborgen.

In alle scenario's zien we op het moment dat Blockchain wordt geïmplementeerd in de financiële administratie van een organisatie dat het zwaartepunt van het controleproces naar voren toe zal verschuiven. Hierdoor wordt het mogelijk een vorm van continuous auditing te gaan toepassen, waardoor de huidige vorm van de jaarrekeningcontrole overhoop wordt gehaald.

5 Beantwoording centrale vraagstelling

Het doel van dit onderzoek is om meer inzicht te verschaffen in de impact van blockchain technologie op het controleproces van de accountant. De centrale onderzoeksvraag die is geformuleerd is: *Op welke wijze wordt het controleproces van de accountant beïnvloed door de implementatie van blockchain technologie bij organisaties*?

Kijkend naar de huidige controlewerkzaamheden van de accountant in het kader van de jaarrekening, zijn de controlewerkzaamheden gericht op de standen en stromen van de opgestelde jaarrekening key. Vanuit het perspectief van blockchain zijn er op het moment dat organisaties blockchain applicaties gaan gebruiken een aantal kansen om het controleproces efficiënter en effectiever te maken, maar waarbij het belangrijkste voordeel is dat de kwaliteit van de gehele controle omhoog kan. Naast deze beheersingsmaatregelen, die veel klassieke risico's wegnemen, zijn er ook een aantal risico's te benoemen die gerelateerd zijn aan blockchain technologie. Deze risico's zal de accountant moeten onderkennen en daarop zijn controlewerkzaamheden afstemmen. De risico's zijn in te kaderen in de volgende categorieën:

- Data gerelateerde risico's;
- Beveiligings, privacy en compliance risico's;
- Gedrags- en kennis risico's

In de conclusie van deze scriptie zijn een aantal scenario's geschetst op welke wijze het inhoudelijke controleproces zou kunnen gaan wijzigen op het moment dat blockchain is geïmplementeerd bij de te controleren organisaties. Hiermee wordt ook de centrale vraag beantwoordt *(Op welke wijze wordt het controleproces van de accountant beïnvloed door de implementatie van de blockchain technologie bij organisaties?)* Uit de scenario's kan geconcludeerd worden dat op dit moment het niet duidelijk aan te geven is, op welke wijze het controleproces van de accountant inhoudelijk wordt beïnvloed. De wijzigingen zullen afhankelijk zijn van een aantal variabelen die in de nabije toekomst vorm dienen te krijgen.

Wel kan de volgende conclusie worden getrokken met betrekking tot blockchain in relatie tot de accountant; De accountant zal verantwoordelijk blijven voor het geven van zekerheid bij het te controleren object, dit hoeft echter niet de jaarrekening te betreffen in de toekomst. De verschillende fases van het controleproces blijven naar alle waarschijnlijkheid gehandhaafd maar de uitvoeringsfase zal er anders uit komen te zien. Het aantal gegevensgerichte werkzaamheden zal afnemen en het zwaartepunt van de controle zal liggen bij de controle op de input van een blockchain (ofwel smart contracts) en de opbouw van de blockchain zelf. Hierdoor wordt continuous auditing mogelijk doordat de technologie, blockchain, beheersingsmaatregelen in zich heeft, zoals: decentralisatie, transparantie, on-aanpasbaarheid en anonimiteit. Het is nog onduidelijk of de accountant deze controlewerkzaamheden rondom blockchain zelf gaat uitvoeren of hiervoor specialisten zal inschakelen.

6 Bibliografie

Alles, M. G. (2015, Juni). Drivers of the Use and Facilitators and Obstacles of the Evolution of Big Data by the Audit Profession. *Accounting Horizons, Vol. 29 Issue*, pp. 439-449.

Avexo. (2017). *uitleg-blockchain-technologie*. Opgeroepen op februari 4, 2017, van www.uitlegblock-chain: https://www.uitlegblockchain.nl/uitleg-blockchain-technologie/

Bader, R., & Thorsten, D. (2017, april 25). *CIO*. Opgeroepen op juni 2, 2017, van hoe de blockchain werkt: http://cio.nl/netwerken/98367-hoe-de-blockchain-werkt#

Bolt, M. (2015). *Wat is blockchain*. Opgeroepen op mei 23, 2017, van www.watisblockchain.nl: http://www.watisblockchain.nl/wat_is_blockchain.php

Bolt, M. (2017, feb 24). *blockchain*. Opgeroepen op 2 24, 2017, van www.martijnbolt.com: http://www.martijnbolt.com/nl/blockchainnl/

Bolt, M. (sd). *Wat is blockchain*. Opgeroepen op maart 20, 2017, van http://www.watisblock-chain.nl/wat_is_blockchain.php:

Bruin de, L. (2016, oktober). Een compactere overheid door de blockchain. *Ibestuur*.

CGMA. (2017). *blockchain decentralised ledger system*. Opgeroepen op mei 23, 2017, van http://www.cgma.org/magazine/2017/jun/blockchain-decentralised-ledger-system.html

EY. (2017). *blockchain voorbij de hype*. Opgeroepen op mei 23, 2017, van http://www.ey.com/nl/nl/indu-stries/financial-services/banking---capital-markets/ey-blockchain-voorbij-de-hype

ING. (2015). brancherapport accountancy. Amsterdam, Nederland.

Kelly, B. (2015). The Bitcoin big bang: how alternative currencies are about to change the world. Hobo-ken, N.J.: John Wiley & Sons.

morgen, a. v. (2017). *blockchain is echt blijvertje*. Opgeroepen op april 28, 2017, van http://www.accoun-tancyvanmorgen.nl/2017/06/26/blockchain-is-echt-blijvertje-blockchain-ook-zonder/

Pinna, A. &. (2016). *Distributed ledger technologies in securities post trading.*

Pomp, M., & Hartog , K. (2017). *blockchain magazine.* Opgeroepen op maart 9, 2017, van www.block-chainpilots.nl/blockchain-magazine#!/digicommissaris-bas-eenhoorn

Roorda, B. (2016). *Zeven vragen over blockchain*. Opgeroepen op 2 24, 2017, van https://www.accoun-tant.nl/artikelen/2016/3/zeven-vragen-over-blockchain/

Rückeshäuser, N. (2017). Do we really want blockchain-based accounting? Decentralized consensus as enabler of management override of internal controls. *International Conference on Wirtschaftsinformatik*, (pp. 16-30). St. Gallen: Switzerland.

Schep, T. (2017, juli). *blockchain*. Opgeroepen op juli 11, 2017, van technologiebeleid: https://www.technologiebeleid.nl/blockchain/

Schwab van, K. (2016). *The fourth industrial revolution.* World Ecnomic Forum.

Van de Velde, J. S. (2016). *Blockchain in Capital Markets, the prize and the journey.*

Vigna, P. &. (2015). The age of cryptocurrency : how bitcoin and digital money are challenging the global economic order. New York: St. Martin's Press.

Vos, M. (2017, April). Blockchain leert vooral anders kijken. *Ibestuur*, pp. 60-63.

Voskuilen, O. (2017, 01 30). *Herdefiniëring van control – Blockchain*. Opgeroepen op februari 4, 2017, van FM: http://financieel-management.nl/artikel/herdefiniering-van-control--blockchain

wikipedia. (sd). *wikipedia*. Opgeroepen op maart 24, 2017, van https://nl.wikipedia.org/wiki/Blockchain: https://nl.wikipedia.org/wiki/Blockchain

Zuidam, r. (2016). *Government-as-a-Service: Het nieuwe Nederlandse exportproduct* . Dutchchain.

Business Intelligence Tooling bij jaarrekeningcontroles

Aram Falticeanu

Aram Falticeanu is als audit-trainee begonnen bij KPMG in 2009 en is als tech-savvy auditor doorgegroeid tot MT-lid binnen de afdeling Digital Assurance & Innovation (DANÍ). Als MT-lid heeft Aram development en science & technology in zijn de portefeuille. Technologie in de audit heeft ook altijd een belangrijke rol gespeeld bij zijn controleopdrachten. Na het behalen van de titel registeraccountant heeft Aram zich verder verdiept in digitalisering binnen het audit-domein. Om zijn kennis te verrijken vanuit een academisch perspectief is hij als eerste lichting begonnen met het executive program digital auditing aan de Vrije Universiteit van Amsterdam. Hier heeft hij alle fases (basic, advanced en het expert programma) nominaal doorlopen, waarmee hij uitgebreide kennis heeft verkregen met betrekking tot het doorgronden van technologie vanuit een audit-perspectief. Deze kennis zet hij in om de controlepraktijk te innoveren bij KPMG via DANÍ. Als onderdeel van het expert programma heeft hij zich aangesloten bij het laatste jaar van de IT Audit Compliance and Advisory opleiding en daarbij een afsluitend scriptieonderzoek uitgevoerd. Zijn scriptie geeft inzicht in de aanpak van auditinnovaties waarbij specifiek wordt ingegaan op het ontwikkelen van Business Intelligence Tooling binnen de controlefase van jaarrekeningcontroles en hoe deze ontwikkeld kan worden aan de hand van best practices.

1 Inleiding

Hoe de jaarrekeningcontroles wordt uitgevoerd of waarom bepaalde gebeurtenissen niet zijn gesignaleerd wordt anno 2018 in diverse mediaberichten kritisch belicht. In het boek The Auditor: Quo Vadis? van Mervyn King en Linda de Beer (2018) worden de mogelijke gevolgen hiervan scherp neergezet: 'Without significant innovation in its business model, staff recruitment strategies and audit execution processes, the audit profession may not remain relevant in the 21st century'. Voor de uitvoering van het audit proces kan dit mijns inziens veranderen door geavanceerde IT-hulpmiddelen in te zetten.
De te ontwikkelen oplossingen voor de controlepraktijk moeten zorgen voor meer focus en effectievere jaarrekeningcontroles en minder administratieve lasten. De controlerend accountant dient vanuit wet- en regelgeving zijn controledossier dusdanig in te richten dat dit zelfstandig leesbaar is voor een goed geïnformeerde derde. Uit dit controledossier moet blijken dat voldoende werkzaamheden uitgevoerd zijn waaruit blijkt dat het oordeel in de verstrekte controleverklaring passend is geweest. Om dit te bewerkstelligen worden overwegingen bijvoorbeeld met betrekking tot de risico-inschatting gedurende de planningsfase in diverse administratiesystemen, notities, werkprogramma's, notulen van besprekingen, etc. vastgelegd. Deze pluriformiteit zorgt voor een arbeidsintensieve vastlegging waarbij inconsistenties en trends zeer beperkt te detecteren zijn.
Een van de oplossingen bevindt zich nu in de designfase als onderdeel van de PoC -fase. Het doel is om vanuit verschillende systemen informatie te bundelen om de kwaliteit van de te gebruiken gegevens te verhogen, de doelgerichtheid van controleteams te verhogen en door middel van nieuwe inzichten toegevoegde waarde te bieden aan de controleteams. De te ontwikkelen applicatie gaat globaal als volgt werken:

1 De data wordt vanuit verschillende bronnen verzameld en waar mogelijk in combinatie met robotica overgenomen in de applicatie.
2 De verzamelde data wordt gestructureerd tot één database.
3 In de applicatie wordt de data middels verschillende query's geautomatiseerd gevalideerd en attentiepunten worden zichtbaar gemaakt middels kunstmatige intelligentie.
4 Via een dashboardfunctie worden de uitkomsten van de verzamelde en geanalyseerde gegevens gepresenteerd. Door passende parametrisering wordt de gebruiker risicogericht en aangepast naar het functieniveau van de betreffende medewerker geïnformeerd. Vanuit deze weergave kan altijd de gedetailleerde informatie geraadpleegd worden. Bij de inrichting is aandacht besteed aan beveiliging van deze gegevens en de inrichting van de juiste functiescheiding.
5 Het is de taak van het individuele controleteam om de documentatie te controleren en waar nodig aan te vullen alvorens zij de informatie accepteren. De gecontroleerde en geaccepteerde informatie wordt geautomatiseerd gereedgemaakt ten behoeve van verzending naar het controledossier.
6 De output uit de vorige stappen wordt (geautomatiseerd) opgenomen in het controledossier.

(Figuur 1 grafische weergave aanleiding – eigen ontwerp)

Deze oplossing gaat ingezet worden in het kader van de jaarrekeningcontrole en moet voor de gebruiker werken als Business Intelligence Tooling (hierna: BI-Tooling).

2 Theoretisch kader

2.1 Inleiding

In het kader van deze publicatie wordt in dit hoofdstuk een verkorte versie van het theoretisch kader weergegeven. Hiermee wordt de eerste deelvraag 'Aan welke voorschriften en richtlijnen moet voldaan worden om verkregen inzicht vanuit een BI-Tooling te kunnen gebruiken in het kader van de jaarrekeningcontrole en welke risico's zijn hierbij te onderscheiden?' beantwoord.

2.2 Literatuur/Theorie

2.2.1 Definitie BI

Het verkrijgen van een begrijpelijke definitie van BI-Tooling is relevant om te begrijpen wat de ontwikkeling moet bewerkstelligen. Om de definitie te bepalen heb ik vanuit de verscheidenheid aan uitleg over de definitie van Business Intelligence vier verschillende autoriteiten binnen het IT -auditdomein geselecteerd met complementeren definities. Hieronder heb ik de vier verschillende definities weergegeven:

1 In de IT-woordenlijst van Gartner (2018) wordt Business Intelligence als volgt beschreven: "BI is een kapstokterm waaronder applicaties, infrastructuren, hulpmiddelen en aanbevolen werkwijzen vallen die toegang geven tot het analyseren van gegevens om beslissingen en prestaties te verbeteren en te optimaliseren."
2 Forrester (2018) definieert Business Intelligence als een reeks aan methodologieën, processen, architecturen en technologieën die de output van managementinformatie gebruikt voor analyses, rapportages, prestatiemanagement en informatieverstrekking.
3 ISACA (2018) geeft in de eigen woordenlijst geen definitie van Business Intelligence. Tijdens een van de gepubliceerde ISACA events geeft Matt Schwartz (2011) zijn definitie: "Business Intelligence zorgt ervoor dat organisaties op feiten gebaseerde beslissingen kunnen nemen. Deze beslissingen kunnen genomen worden door de onderliggende data te aggregeren, te visualiseren en te verrijken alvorens een weloverwogen beslissing genomen kan worden."
4 The Data Warehouse Institute (2018) (hierna: TDWI) geeft aan dat BI-Tooling ervoor moet zorgen dat niet-technische gebruikers binnen een organisatie direct toegang krijgen tot data en zelf inzichten kunnen verkrijgen uit de data. Hierbij geven zij aan dat de toegang tot de data wordt verzorgd door een set aan tools die ervoor moeten zorgen dat gebruikers zonder tussenkomst van een data scientist of IT'ers data kunnen raadplegen.

Vanuit bovenstaande vier bronnen is Business Intelligence als volgt gedefinieerd: Business Intelligence zorgt voor een gestructureerd proces waarbij de gebruiker wordt gefaciliteerd bij het nemen van de juiste beslissingen. Hierbij wordt de gebruiker geïnformeerd over de reeds ingevulde data en heeft de gebruiker de mogelijkheid om data te verrijken alvorens een weloverwogen beslissing genomen kan worden.
Tooling is vanuit gangbare IT-definities bekend als een term voor hulpprogramma's die voor gebruikers bepaalde handelingen overneemt of vereenvoudigt. Uit onder andere het online woordboek van Cambridge (2018) komt naar voren dat het hulpmiddelen zijn voor een specifiek doel en dat het gebruikt wordt als gereedschap om te komen tot het specifieke doel. In de online Van Dale (2018) wordt tooling uitgelegd als hulpmiddel bij het werk (bijvoorbeeld een computerprogramma). Het gaat dan bijvoorbeeld om een ondersteunende applicatie. Voor deze casestudy maakt de tooling Business Intelligence mogelijk waardoor gesproken wordt over BI-Tooling. Kortom: de BI-tooling zorgt voor een gestructureerd proces waarbij de gebruiker wordt gefaciliteerd bij het nemen van de juiste beslissingen.

2.2.2 Voorschriften, richtlijnen en toetsingsnormen

De Koninklijke Nederlandse Beroepsorganisatie van Accountants (hierna: NBA) stelt de voorschriften en richtlijnen voor accountants vast. In de Handleiding Regelgeving Accountancy (hierna: HRA) zijn de nadere voorschriften controle- en overige standaarden (hierna: NV COS) opgenomen. Vanuit de NV COS is de accountant in het kader van de jaarrekeningcontrole verplicht om in bijvoorbeeld de planningsfase rekening te houden met risico's op een afwijking van materieel belang. De accountant dient de controle zodanig te plannen dat deze op een effectieve wijze zal worden uitgevoerd. Beide punten zijn in NV COS 300 en 315 nader uitgewerkt. Hierin staan geen beperkingen voor het gebruik van BI-Tooling. Hierin wordt vooral beschreven wat het uiteindelijke doel is en niet hoe je daar moet komen. Het gebruik van auditsoftware zoals BI-Tooling is toegestaan en deze moet dan bijdragen aan het einddoel. In de hele HRA 2018 komt de term 'auditsoftwaretoepassingen' overigens maar achttien keer voor verdeeld over de volgende standaarden:

NV COS	Standaard
240	De verantwoordelijkheden van de accountant m.b.t. fraude in het kader van een controle van financiele overzichten.
300	Planning van een controle van financiële overzichten
330	Inspelen door de accountant op ingeschatte risico's
505	Externe bevestigingen

(Figuur 2 weergave NV COS-standaarden – eigen ontwerp)

Bovenstaande komt in mindere mate voor in de Gedrags- en Beroepsregels van NOREA (2018) voor RE's. Vanuit de regelgeving voor RA's en RE's worden geen beperkingen opgelegd ten aanzien van het gebruik van auditsoftwaretoepassingen of specifieker BI-Tooling. Dit wordt ondersteund door Eimers, P., & Amerongen, A. (2015). Zij geven aan dat de controlestandaarden zijn gebaseerd op principes en dat deze standaarden voldoende ruimte bieden aan de accountant om voldoende en geschikte controle-informatie te verzamelen in een combinatie van systeem- en gegevensgerichte werkzaamheden. Als voorbeeld geven zij dat data-analyse niets anders is dan een nieuw/verbeterd hulpmiddel om te voldoen aan regelgeving.
In het kader van dit onderzoek is de BI-Tooling aangemerkt als auditobject en dit wordt beoordeeld aan de hand van een toetsingsnorm naast best practices. Voor softwareontwikkeling kan Projects in Controller Environments (hierna: PRINCE2) gehanteerd worden als toetsingsnorm door IT-auditors. Deze toetsingsnorm moet geconcretiseerd worden naar de praktijkomgeving om te kunnen fungeren als normenkader voor BI-Tooling. De verdere concretisering zorgt ervoor dat in dit onderzoek op een professionele wijze een IT-audit uitgevoerd en gedocumenteerd kan worden. Het te toetsen aan deze erkende norm zal bijdrage aan de kwaliteit van deze softwareontwikkeling. Het enkel toepassen van PRINCE2 is niet voldoende volgens Breij & Havinga (2014) aangezien echt samengewerkt moet worden; derhalve is gezocht naar een aanvullend model. Gelijktijdig vragen de huidige complexiteit van de gewenste BI-Tooling en de snelle technologische ontwikkelingen om een iteratieve ontwikkelcyclus. Het combineren van PRINCE2 met een Agile werkmethode tijdens de implementatiefase zorgt voor een effectievere softwareontwikkeling (Sommer et al., 2015). In combinatie met andere best practices kan een antwoord gevonden worden op de centrale vraagstelling en deelvragen in het kader van dit onderzoek.
De ontwikkeling van deze BI-Tooling ter ondersteuning van de jaarrekeningcontrole vindt plaats in een sterk gereguleerde omgeving. Ervoor zorgen dat de BI-Tooling de juiste vaktechnische stappen doorloopt om een passende uitkomst te kunnen genereren is vooral een afstemming tussen bureau vaktechniek en het ontwikkelteam. Beide partijen streven naar doeltreffendheid en doelmatigheid; PRINCE2 (2018) is een projectmanagementmethode gericht op het gestructureerd uitvoeren van projecten en wordt bij softwareontwikkelprojecten gehanteerd als toetsingsnorm ten behoeve van kwaliteitsbewaking. Het toepassen van PRINCE2 alleen is niet voldoende (Breij en Havinga, 2014). Om het succes van de ontwikkeling van de BI-Tooling te vergroten is gezocht naar aanvullende best practices welke in paragraaf 2.2.4. nader zijn uitgewerkt.

2.2.3 Risico's tijdens implementatie van BI-Tooling

Het verkrijgen van inzicht door middel van BI-Tooling in het kader van de jaarrekeningcontrole is een nieuwe manier van werken binnen een accountantskantoor. In het onderzoeksartikel van Cohen et al.. (1979) wordt aangegeven dat de organisatiestructuur verandert door innovatietechnologieën. Het gebruik van BI-Tooling kan geclassificeerd worden als een dergelijke innovatietechnologie. Cohen geeft aan dat het gebruik van zulke innovatietechnologie sterk afhangt van het gedrag en de handelingen van management. Omoteso (2014) geeft aan dat besluitvormingshulpmiddelen of beslissingsondersteunende systemen worden ontwikkeld door de grotere accountantskantoren. Het hoofddoel van deze technische hulpmiddelen is om de accountant te ondersteunen bij het nemen van betere beslissingen. Dit is mogelijk door vooroordelen en omissies vanuit een regulier beslissingsproces te adresseren vanuit technische oplossingen. Deze twee constateringen heb ik meegenomen in het onderzoek naar de verschillende risico's.

In wetenschappelijke literatuur, zijnde peer reviewd artikelen, is informatie over BI-Tooling beperkt beschikbaar. Op basis van de publicatiedata lijkt dit te worden veroorzaakt doordat het inzetten van BI-Tooling een relatief nieuwe werkwijze betreft. Om risico's tijdens de implementatie van BI-Tooling nader te onderzoeken vanuit wetenschappelijk perspectief zijn eerst de risico's bij softwareontwikkelprojecten onderzocht, aangevuld met professionele literatuur gericht op het IT-domein.

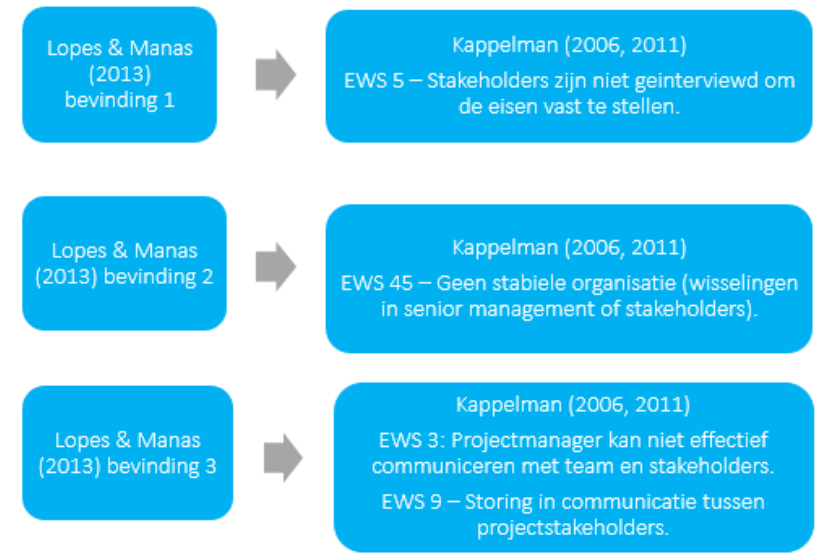
In verschillende onderzoeken wordt door de onderzoekers gesproken over risico's en attentiepunten bij softwareontwikkelprojecten. De complexiteit van het maken van een passende inschatting van het softwareproject wordt door Stutzke (2005) als risico gezien. Voor het softwareproject moeten de mensuren en doorlooptijd bepaald worden. Het maken van deze inschatting, het adequaat plannen van bijbehorende middelen en het meten van de voortgang zijn complex. Hierdoor kan management de totale projectkosten, het rendement op de investering en de kwaliteit en time to market moeilijk beheersen. Dit risico wordt door Trendowicz & Jeffery (2014) als een van de oudste en belangrijkste problemen bij het managen van softwareprojecten gezien. Kranenburg (2008) geeft vanuit softwareontwikkeling aan dat zonder een toegewijd ontwikkelteam het niet ongebruikelijk is dat deze projecten worden uitgevoerd door de beschikbare medewerkers en niet door de medewerkers met de juiste capaciteiten. Dit risico wordt door Reifer (2002) herkend en onderverdeeld in risico's van technische en leidinggevende aard. Risico's moeten worden geïdentificeerd en vervolgens moet de risicobereidheid bepaald worden. Afhankelijk van de risico-inschatting en risicoacceptatie kan het risico gemitigeerd of geaccepteerd worden. Als hierbij onderscheid gemaakt wordt tussen technische en organisatorische potentiële risico's en deze conform de risicobereidheid worden behandeld, dan is de basis voor een succesvol softwareontwikkelproject gelegd.

Deze risico's en attentiepunten kunnen voorafgaande aan het project of tijdens het project ontdekt worden. Kappelman (2006, 2011) heeft meerdere studies uitgevoerd waarin hij spreekt over Early Warning Signs (EWS). Dit betreffen de vroegtijdige waarschuwingssignalen of attentiepunten die duiden op risico's voor mislukkingen binnen het IT-project. In het onderzoek van Kappelman & Zhang (2006) en Kappelman (2011) hierna Kappelman (2006, 2011) worden 53 EWS benoemd en wordt een splitsing gemaakt tussen risico's gerelateerd aan het menselijke en het procesmatige aspect van een IT-project. Vroeg in de ontwikkelcyclus kunnen EWS worden ontdekt en kunnen passende maatregelen genomen worden. Doordat vroegtijdig kan worden bijgestuurd of besloten kan worden om te stoppen zijn deze IT-projectrisico's relevanter dan generieke IT-projectrisico's. Onderzoek van Bi (2009) ondersteunt deze visie en benadrukt dat een interne audit gericht op procesrisico's in een IT-project kan voorkomen dat een project faalt. De bijbehorende gedachte is vergelijkbaar met de EWS van Kappelman. Bi (2009) geeft vooral aan dat het systematisch uitvoeren van een controlemechanisme relevant is om op koers te blijven richting het einddoel van het IT-project. Het onderzoek van Lopes & Manas (2013) geeft aan dat gebrek aan stakeholdermanagement de opleveringsdeadline van het project negatief kan beïnvloeden. Hierbij worden drie specifieke gebreken benoemd:

1 Het niet kunnen identificeren van een of meerdere stakeholders voor het IT-project bij aanvang van het project
2 Toevoegen of wijzigen van stakeholders na de start van het project

3 Slechte communicatie tussen IT-projectmanagement en stakeholders. Een gezamenlijk doel ontbreekt waardoor het mislukt om een eenduidige scope van het project te krijgen. Door dit of de gevolgen in de communicatie niet te adresseren loopt het project later in het proces vertraging op. Deze vertraging komt met name doordat de scope later in de ontwikkeling wijzigt na afstemming met de stakeholders.

Als een van de oplossingen wordt een Agile werkmethode aangedragen door Lopes & Manas (2013). Voor het praktijkonderzoek dat plaatsvindt bij een grote onderneming is deze bevinding met betrekking tot gebrekkig stakeholdermanagement zeer relevant. De gebreken met betrekking tot stakeholdermanagement komen op hoofdlijnen overeen met de EWS van Kappelman (2006, 2011) en deze heb ik hieronder met elkaar gekoppeld.



Figuur 3 Lopes & Manas (2013) gekoppeld met Kappelman (2006, 2011) – eigen ontwerp

Uit het onderzoek van Kappelman (2011) komt naar voren dat bijsturing van EWS nodig is om het slagen van IT-projecten te vergroten. Het onderzoek van Lopes & Manas (2013) gaf al aan dat een Agile werkmethode hierbij kan ondersteunen; derhalve zal bij het praktijkonderzoek Agile ontwikkeld worden. In de volgende paragraaf is de ontwikkelmethode gekoppeld aan een model en nader uitgewerkt.

2.2.4 Model voor implementatie BI-Tooling

Het doel van BI-Tooling is om data uit verschillende bronnen te combineren en te structureren ten behoeve van de organisatie. Met deze inzichten kunnen door BI-Tooling in een korte tijdsperiode inzichten worden verstrekt als managementinformatie (Horáková & Skalsa, 2013). Dit komt overeen met de geformuleerde definitie in paragraaf 2.2.2. Uit de voorgaande paragrafen blijkt dat er geen wondermiddel is om alle risico's bij softwareontwikkeling te mitigeren en dit werd al onderkend door Brooks (1987). Een van zijn suggesties is om de risico's op te delen in inherente uitdagingen bij softwareontwikkeling en vervolguitdagingen na implementatie die niet inherent zijn aan de softwareontwikkeling. Voor dit onderzoek is verder gezocht naar succesfactoren en een bijbehorend model om deze constateringen te adresseren.
Uit verschillende onderzoeken blijkt dat succesvolle implementatie van BI-Tooling afhangt van organisatie- en sectorspecifieke factoren. Het onderzoek van Dyba et al. (2015) geeft vier principes van Agile projectmanagement weer die bijdragen aan een succesvolle softwareontwikkeling. De vier principes zijn minimale

zwaarwegende specificaties, autonome teams, redundantie in teams en continu leren door middel van feedback. Vanuit het onderzoek van Trijssenaar & Zalm (2013) is een normenkader opgesteld om toepassing van Agile in de praktijk te toetsen.

Onderdeel Agile proces	Principes (Dyba et al) ten behoeve van succes	Toetsingselementen (Trijssenaar en Zalm) succesvolle toepassing
Agile-ontwikkeldocumentatie	Minimale zwaarwegende specificaties	Verzamelde eisen en wensen in use cases, vaststellen aanwezigheid, accordering en format
		Burndown chart, aanwezigheid en weergave actuele standen
Werking Agile-proces	Continu leren door middel van feedback	Planning van de iteraties overleggen
		Backlogs iteraties
		Retrospectief deel van sprint overleg
Randvoorwaarden team in Agile-proces	Autonome teams inclusief redundantie in teams	Vertegenwoordiging senior staff zijnde product owner van de BI-Tooling
		Team samenstelling kennis en ervaring
		Communicatie tussen Agile team en product owner
Inzet middelen ten behoeve van project	Combinatie minimale zwaarwegende specificaties en autonomen teams	Geleverde functionaliteiten in timeboxen
		Geleverde functionaliteiten met aantal mensuren ter indicatie van kwaliteit

(Figuur 4 Agile proces gekoppeld met Dyba et al.-principes en toetsingselementen van Trijssennaar & Zalm – eigen ontwerp)

De projectmethode PRINCE2 zoals weergegeven in paragraaf 2.2.2. van dit scriptieonderzoek alleen is niet voldoende (Breij en Havinga, 2014). Een succesvol project heeft baat bij een gestructureerde aanpak ondersteund door tools en methodieken (Keuningen & De Meijer, 2016). Daarom is deze projectmethode gekoppeld aan de hierboven weergegeven Agile werkmethode voor een effectievere softwareontwikkeling (Sommer et al., 2015). Dit is hieronder in een model voor de ontwikkeling van de BI-Tooling weergegeven. Dit kan de kwaliteit van deze softwareontwikkeling ten goede komen, door per fase de verschillende componenten van PRINCE2 te koppelen met Agile. Hiermee kunnen deze elementen tijdens het praktijkonderzoek getoetst worden aan de praktijk.

Projectfase	PRINCE2 Hoofdproces(sen)	PRINCE2 Thema(s)	Onderdeel Agile proces	Onderdeel Agile proces
Voorbereiden en starten ontwikkelproject	Opstarten	Plannen, risico, organisatie, businesscase.	Randvoorwaarden team in Agile proces en Agile-ontwikkeldocumentatie	Voorbereiding en starten sprint
	Initiëren van het project	Plannen, kwaliteit, risico, businesscase.	Agile-ontwikkeldocumentatie	Iteratie(s)
Uitvoering ontwikkelproject	Beheersen van een fase	Voortgang, wijziging	Inzet middelen ten behoeve van project	Iteratie(s)
	Managen van opleveren ontwikkel-producten	Wijziging, kwaliteit, voortgang	Werking Agile proces	Iteratie(s)
	Managen van mijlpalen	Risico, Voortgang	Inzet middelen ten behoeve van project en Werking Agile-proces	Iteratie(s)
Afsluiting ontwikkelproject	Formeel sluiten van het ontwikkelproject	Kwaliteit, Businesscase	BI-Tooling is in productie en monitoren gebruik incl. start versie 2	Einde van alle iteraties in sprint

(Figuur 5 PRINCE2 gekoppeld met Agile – eigen ontwerp)

Op basis van het onderzoek van Mesaros et al. (2016) zijn tien gebieden geïdentificeerd waaraan aandacht besteed dient te worden om de succeskans te vergroten. Dit komt grotendeels overeen met de geformuleerde risicofactoren in paragraaf 2.2.3. van dit scriptieonderzoek. Het onderzoek van Mesaros inclusief het bijhorende model is na peer-review gepubliceerd in Journal of Systems Integration. In het praktijkonderzoek wordt dit model gehanteerd als best practice aangezien dit veel raakvlakken heeft met de stakeholderdynamiek die van toepassing is bij de organisatie waar de casestudy uitgevoerd zal worden. Hieronder is het model van Mesaros weergegeven.

(Figuur 6 Model succesfactoren Mesaros et al. (2016))

In het model worden tien succesfactoren weergegeven die op basis van het statistische onderzoek bijdragen aan succesvolle implementatie en verder gebruik van BI-Tooling. Hierbij hebben de succesfactoren betrekking op twee focusgebieden: de technologie of het personeel en de organisatie. In het praktijkonderzoek heb ik specifiek aangegeven hoe ik het model van Mesaros et al. (2016) heb gehanteerd om de risico's in het praktijkonderzoek te mitigeren. Tevens zal ik daarbij de EWS van Kappelman (2011) bespreken voor het praktijkonderzoek.

2.2.5 Platformen voor BI-Tooling

Als de visie, de doelstellingen en de initiële omvang van het BI-project bekend zijn, moet bepaald worden welk platform hiervoor gebruikt zal worden. De markt voor platformen waarop BI-Tooling uitgevoerd kan worden is groot. In het kader van dit onderzoek heb ik de grootste platformen en de gebruikte platformen door de grote accountantskantoren onderzocht. In het artikel van Gartner (2018) , geschreven door Howson et al. (2018), worden 20 topleveranciers besproken die BI-Tooling via platformen aanbieden. Hierbij is sprake van een toename in cloudgerichte platformen welke eenvoudig aangeschaft kunnen worden. Traditionele oplossingen zijn geüpgraded met data-analytische hulpmiddelen en geheel nieuwe oplossingen zijn ontwikkeld binnen de platformen.
Bredere uitrol van uitgebreidere data-analytische hulpmiddelen in combinatie met machine learning wordt vanaf 2020 verwacht. Voor de huidige periode onderkennen Howson et al. (2018) in het Gartner-artikel welke sterke punten en attentiepunten per leverancier van BI-platformen te onderkennen zijn.
De uitkomsten hiervan zijn geplot en grafisch weergegeven in de volgende tabel. Op de Y-as zijn de uitvoeringsmogelijkheden weergegeven en op de X-as volledigheid visie, waarbij gekeken is of in de roadmap aangegeven wordt wanneer (nieuwe) technologieën worden toegevoegd aan het platform.

Source: Gartner (February 2018)

(Figuur 7 Analyse BI-Platformen Howson et al. (2018) Gartner artikel)

Opvallend hierbij is dat Qlik, Tableau en Microsoft worden gebruikt door een deel van de grotere accountantskantoren en dat deze rechtsboven in het kwadrant staan. PwC, Deloitte en KPMG maken gebruik van de drie partijen die het kwadrant 'leaders' vormen. Op basis van openbare informatie (KPMG, 2018-1) is bekend dat KPMG voor klanten gebruikmaakt van het KPMG SOFY-platform, een geavanceerde BI-Tool gericht op supply chain, compliance, procurement en tax. De tool helpt organisaties om informatie te ontsluiten en relevante analyses op te stellen zodat de juiste beslissing genomen kunnen worden. Het SOFY-platform heeft raakvlakken met het platform van Microsoft aangezien het SOFY-platform gebruikmaakt van Microsoft Azure-technologie (KPMG, 2018-1). In paragraaf 3.1. wordt nader uitgewerkt waarom het praktijkonderzoek is gebouwd binnen het SOFY-platform. Een van de belangrijkste redenen was dat de keuze voor een BI-platform niet een losstaand softwarepakket betreft dat geselecteerd wordt (van der Waa & Griffioen, 2013).

2.3 Beantwoording eerste deelvraag

Als sluitstuk van het theoretisch kader wordt de eerste deelvraag beantwoord en worden kort de modellen weergegeven die in de casestudy getoetst zullen worden. De eerste deelvraag 'Aan welke voorschriften en richtlijnen moet voldaan worden om verkregen inzicht vanuit een BI-Tooling te kunnen gebruiken in het kader van de jaarrekeningcontrole en welke risico's zijn hierbij te onderscheiden?' kan op basis van de

voorgaande paragrafen beantwoord worden. Formeel gezien zijn er vanuit voorschriften en richtlijnen geen beperkingen om BI-Tooling in te zetten. De BI-Tooling kan als ondersteunend hulpmiddel worden ingezet bij de jaarrekeningcontrole.
De risico's die onderkend zijn hebben betrekking op de ontwikkeling van de BI-Tooling alvorens deze ingezet kan worden in het kader van de jaarrekeningcontrole. Grofweg worden twee groepen aan risico's onderkend: technische- en projectmatige risico's. Om beide risicogroepen te mitigeren tot een acceptabel niveau zijn een aantal modellen onderkend vanuit de literatuur. In deze modellen (Kappelman 2011, Mesaros et al., 2016) worden een aantal succesfactoren en vroegtijdige waarschuwingssignalen of attentiepunten onderkend. Tevens wordt onderschreven dat een Agile werkmethode hieraan kan bijdragen (Lopes & Manas, 2013). Deze inzichten vanuit de theorie worden meegenomen in het praktijkonderzoek. Kortom: inzet van BI-Tooling in het kader van de jaarrekeningcontrole is op basis van het theoretisch onderzoek mogelijk. De projectmatige en beproefde basis van PRINCE2, de succesfactoren van het model van Mesaros en een iteratieve ontwikkelmethode van Agile zorgen gecombineerd voor een solide softwareontwikkeling. Om vast te stellen dat de Agile ontwikkelmethode succesvol wordt toegepast wordt het model van Dyba et al. (2015) en Trijssenaar & Zalm (2013) gecombineerd gehanteerd.

3 Case study

In het kader van deze publicatie wordt in dit hoofdstuk een verkorte versie van de casestudy weergegeven waarbij de modellen zijn getoetst in de praktijk. Dit vormt de basis voor de verdere analyse in hoofdstuk 4 waarmee de tweede deelvraag 'Welke mitigerende controlemaatregelen worden in de praktijk genomen door de accountantsorganisatie met betrekking tot risico's bij de inzet van BI-Tooling met betrekking tot opzet, bestaan en werking?' wordt beantwoord. Om dit te bereiken wordt eerst in dit hoofdstuk de omgeving waar de casestudy is ontwikkeld beschreven. Gelijktijdig worden de functionaliteiten van de BI-Tooling beschreven. Hiermee wordt inzicht gegeven in de relevantie van de ontwikkeling en in wat de BI-Tooling doet.

3.1 Situatiebeschrijving

De BI-Tooling wordt ontwikkeld voor KPMG, een van de Big4 accountantskantoren. De auditpraktijk binnen de organisatie verricht jaarlijks ongeveer 3.000 jaarrekeningcontroles. Deze worden door diverse controleteams uitgevoerd. De BI-ontwikkeling is erop gericht om accountants van de individuele controleteams te ontlasten bij het uitvoeren de jaarrekeningcontroles. BI-Tooling zorgt voor een gestructureerd proces waarbij de gebruiker wordt gefaciliteerd bij het nemen van de juiste beslissingen. Individuele controleteams zijn verantwoordelijk voor de definitieve besluitvorming in de diverse controlefases. Standaardprocesstappen worden afgedwongen en bij afwijkingen kan de data verrijkt worden waardoor de individuele controleteams een weloverwogen beslissing kunnen nemen.
BI-Tooling is binnen KPMG een verplicht hulpmiddel dat controleteams moeten hanteren om aan te tonen dat zij voldoen aan vaktechnische richtlijnen en eisen vanuit wet- en regelgeving. In de BI-Tooling is een vragenlijst opgenomen die ervoor zorgt dat aan alle aanvullende Nederlandse regelgeving voor jaarrekeningcontroles wordt voldaan indien de vragenlijst juist wordt ingevuld. Vanuit het elektronische controledossier wordt reeds afgedwongen dat aan de internationale regelgeving wordt voldaan. Het omgaan met de hulpmiddelen waaronder de BI-Tooling vraagt wel om een professioneel-kritische houding aangezien onjuist ingevulde vragenlijsten kunnen leiden tot het nemen van onjuiste beslissingen. De accountant is verantwoordelijk voor het eindoordeel, maar afwijkingen moeten worden uitgelegd. Het introduceren van deze BI-Tooling zorgt voor een duidelijker overzicht van de gemaakte keuzes waardoor de kans op het onjuist invullen van de vragenlijst wordt geminimaliseerd. Dit wordt onder andere bereikt doordat gedurende het proces bij veel voorkomende onjuistheden alerts worden aangedragen of doordat extra toelichtingen beschikbaar zijn om definities, etc. nader te definiëren. Tevens geven de alerts aan als bepaalde antwoorden niet gegeven kunnen worden indien dit op basis van de verloopvragen niet is toegestaan. Functioneel zijn er diverse functionaliteiten opgenomen in de BI-Tooling om de bovenstaande beschreven

situatie te realiseren. In het kader van deze publicatie is de weergave van de functionaliteiten en de technische structuur van de BI-Tooling achterwege gelaten.
Voor de situatiebeschrijving van deze casestudy is de selectie van het SOFY-platform als BI-platform relevant. Het platform is eigen BI-platform ontwikkeld door onze consultancycollega's en deze wordt reeds voor andere doeleinden binnen de organisatie gebruikt. Zoals in het theoretisch kader is aangegeven was de keuze voor een BI-platform geen losstaande softwarepakketselectie. Het uitbreiden van de inzetten van het SOFY-platform voor de auditpraktijk was derhalve een eenvoudige keuze.

3.2 Opzet BI-ontwikkeling

Een multidisciplinair team bestaande uit een aanvaarding van de verschillende stakeholders is gevormd om deze softwareontwikkeling te realiseren. In de basis is ervoor gekozen om bij deze ontwikkeling een Agile werkvorm aan te houden. In het theoretisch kader zijn een aantal aandachtspunten, risico's, EWS en succesfactoren benoemd. Bij de opzet van het praktijkonderzoek is rekening gehouden met de volgende aspecten naar aanleiding van het theoretisch kader. Het belang van stakeholdermanager werd door Lopes & Manas (2013) nader uitgewerkt. Het vaststellen van de stakeholders, niet wijzigen van de stakeholders en heldere communicatie zijn meegenomen. Voorafgaande aan de ontwikkeling heeft de ontwikkelafdeling overleg gevoerd met de verwachte stakeholders. Daarna zijn wekelijkse bijeenkomsten gepland om de verschillende stakeholders te informeren en om lopende ontwikkelvragen te bespreken. Tevens hebben wij deze bijeenkomsten gebruikt om eventuele besluiten te nemen.
Het ontwikkelteam heeft een passend tijdschema voor de ontwikkeling gemaakt met behulp van de SOFY-consultants. Zij hebben als consultants ruime ervaring met het plannen van vergelijkbare opdrachten voor onze externe klanten. Om het geheel te managen ben ik zelf aangesteld als projectleider. Om de juiste capaciteiten te hebben binnen het kernontwikkelteam heb ik een Business Analyst met een information management-achtergrond toegevoegd aan het team. Gelijktijdig heb ik een collega vanuit kennismanagement toegevoegd aan het team, wat resulteerde in een toegewijd kernteam met de juiste capaciteiten. Het vormen van het ontwikkelteam en het maken van de tijdsplanning is in lijn met het onderzoek van Trendowicz & Jeffery (2014) en de gedachten van Kranenburg (Kranenburg, 2008) gemaakt.

Uit de literatuur heb ik bij de opzet van deze softwareontwikkeling kennisgenomen van het model van Mesaros. De tien succesfactoren heb ik als projectleider meegenomen bij de aanpak van dit project. Eerst heb ik het model voorgelegd aan de volgende betrokkenen (hierna: stakeholders):

1 Stakeholder A
2 Stakeholder B
3 Stakeholder C
4 Stakeholder D
5 Stakeholder E

Vanuit hun managementrol hebben zij naar verwachting zicht op de verschillende succesfactoren en de toepassing van deze softwareontwikkeling in het grotere geheel. Voor de dagelijkse organisatie zijn zij betrokken bij de processen die gedigitaliseerd gaan worden en bekend met de kwaliteitseisen vanuit de verschillende afdelingen. Na deze interviews, die in paraaf 3.3. nader zijn uitgewerkt, is per succesfactor aangegeven of deze naar verwachting voor dit softwareontwikkelproject bijdragen aan het succes. Halverwege het ontwikkeltraject is een herijking uitgevoerd en nadat de BI-Tool in productie is gebracht heeft nogmaals een evaluatie van het model plaatsgevonden. Gedurende dit gehele traject is er in overleg met de verschillende stakeholders voor gezorgd dat de definitieve BI-Tooling voldoet aan de kwaliteitseisen om gebruikt te kunnen worden in de dagelijkse auditpraktijk. Aanvullende controlemaatgelen om risico's in de opzet, het bestaan en de werking van de BI-Tooling af te dekken zijn vanuit de kwaliteitseisen in combinatie met de succesfactoren overwogen en geïmplementeerd.

3.3 Uitvoering onderzoek en bevindingen

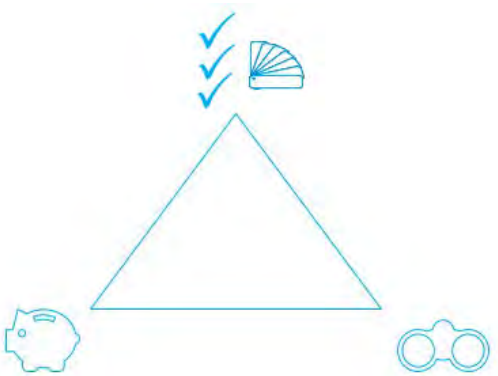
Middels de interviews is het model van Mesaros getoetst. Mesaros stelt dat de tien succesfactoren bij elkaar bepalend zijn voor het succes van het ontwikkelproject. Deze zijn opgenomen in de opzet van het project en verderop in deze paragraaf nader uitgewerkt. Als deze relevant worden geacht door de stakeholders, dan kwalificeren deze ook als de belangrijkste succesfactoren voor dit softwareontwikkelproject. Om zichtbaar te maken in hoeverre de succesfactoren in deze casestudy bijdragen aan het afdekken van de risico's heb ik aan de stakeholders gevraagd om aan te geven wat zij als belangrijkste risico's zien. Vervolgens heb ik gevraagd welke succesfactoren dit kunnen afdekken. In onderstaande tabel zijn de uitkomsten geplot ten opzichte van het Mesaros-model.

Succesfactoren voor BI-Tooling (Mesaros-model)	Stakeholder A	Stakeholder B	Stakeholder C	Stakeholder D	Stakeholder E
1. Visie, Strategie en bedrijfsdoelstellingen	V	-	-	-	V
2. Integratie van BI-Strategie met overall bedrijfsstrategie	-	-	-	-	V
3. Kwaliteit van data	V	V	V	V	V
4. Omvang BI-ontwikkelproject	V	V	-	V	-
5. Segmentatie van oplossingen voor individuele gebruikersgroepen	-	-	-	-	-
6. Projectsponsor	V	V	V	V	V
7. Ondersteuning vanuit top-management	V	V	V	V	V
8. Adequaat team met softwareontwikkelaars	V	-	-	V	-
9. Continue ondersteuning	-	V	V	-	-
10. Open bedrijfscultuur	V	V	V	V	V

(Figuur 8 Plotting Mesaros-model in de praktijk – eigen ontwerp)

Naar aanleiding van de verschillende interviews en bovenstaande plotting van het model van Mesaros voor deze softwareontwikkeling is het interessant om te constateren dat succesfactor 5 door geen van de stakeholders wordt gezien als succesfactor voor het betreffende project. Wel heeft een aantal aangegeven dat dit relevant is voor verdere ontwikkeling. Tevens werd door stakeholder C specifiek aangegeven dat het inregelen van functiescheiding wel wordt gezien als randvoorwaarde binnen het project. Ook is het interessant om te zien dat de strategische, tactische en operationele sturing vanuit de verschillende sta-

keholders terug lijkt te komen in de aangegeven succesfactoren. Ter illustratie: stakeholder A en stakeholder E benoemen de eerste twee succesfactoren die gericht zijn op de strategische niveau. De medeverantwoordelijke voor de uitvoering van de ontwikkeling stakeholder A en stakeholder D benoemen succesfactor 8 die gericht is op het operationele niveau als een belangrijke succesfactor. Hierin herken ik zelf het negenvlaksmodel van Maes (2017). Als de totale plotting wordt bekeken zie je consensus over het belang van vier van de tien succesfactoren deze worden door alle stakeholders onderschreven. Deze richten zich op het neerzetten van een afgewogen BI-Tool gericht op kwaliteit, door samenwerking en ondersteuning vanuit de verschillende gremia.
Voor deze softwareontwikkeling is het interessant om te constateren dat samengevat sprake is van drie focusgebieden. Vanuit de stakeholders komt naar voren dat als de BI-Tool bijdraagt aan auditkwaliteit, het verstrekken van (nieuwe) inzichten en het verbeteren van de werkstroom, dat dan sprake is van een zeer succesvol project. De drie dimensies heb ik als volgt geïnterpreteerd:



(Figuur 9 Dimensies bijdragen softwareontwikkeling - eigen ontwerp)

Vooral vanuit het interview met stakeholder A en stakeholder E, bleek dat efficiency en kostenreductie minder relevant werden gevonden. Hierbij werd kostenbeheersing wel aangehaald als een randvoorwaarde, maar diverse elementen van efficiency werden niet gezien als de belangrijkste succesfactoren voor het project. Als de BI-Tool de auditkwaliteit zou verbeteren en meer of nieuwe inzichten zou verschaffen, dan wordt het project als geslaagd beschouwd. Het uitsluitend investeren in versnelling van het proces c.q. het besparen van tijd als belangrijkste succesfactor zou vanuit het perspectief van de twee stakeholders onvoldoende zijn.

3.3.1 Implementatie Mesaros-model bij uitvoering

Uit de eerste plotting is naar voren gekomen dat de BI-Tooling vooral de auditkwaliteit moet verhogen. Een aantal maatregelen zijn getroffen om de succesfactoren te kunnen implementeren. Hieronder is per succesfactor aangegeven welke maatregelen genomen zijn.

1. Visie, strategie en bedrijfsdoelstellingen

Om onze gezamenlijke visie vorm te geven heb ik eerst bepaald welke initiatieven op hoofdlijnen al onderhanden waren. Vervolgens heeft overleg plaatsgevonden met verschillende gremia, collega's uit het werkveld en de vijf stakeholders aan wie het model van Mesaros is voorgelegd. Door deze gezamenlijke sessie ontstond samenhorigheid en een gedeelde visie. Doordat de omvang van BI-ontwikkelprojecten ook een succesfactor was, bestond de behoefte om de reikwijdte van deze eerste ontwikkeling te beperken. Kortom de scope van eerste ontwikkeling van de BI-Tooling was cruciaal. Als projectleider heb ik voorgesteld om

als eerst een BI-Tooling te ontwikkelen die na afronding gebruikt kan worden door zo veel mogelijk collega's. In overleg met de stakeholders is ervoor gekozen om de vastlegging van het voldoen aan alle Nederlandse wet- en regelgeving in het kader van de jaarrekeningcontrole op te nemen in de BI-Tooling.

2. Integratie van BI-strategie met overall bedrijfsstrategie
Integratie met de overall bedrijfsstrategie is de volgende succesfactor. Het meer toepassen van technologie waaronder BI-Tooling past binnen onze meerjarige bedrijfsstrategie; derhalve hoeft hier geen verdere aandacht aan besteed te worden. De jaarrekeningcontrole efficiënter uitvoeren ontlast de professional. Met dit in het achterhoofd is gekeken naar repeterende werkzaamheden die regelmatig of veelvoudig worden uitgevoerd door de reguliere bedrijfsvoering. Hierbij werden twee significante werkzaamheden geïdentificeerd:

1 De jaarlijkse klant- en opdrachtacceptatie
2 Het per auditdossier vaststellen of aan alle Nederlandse wet- en regelgeving wordt voldaan.

Over deze twee punten is flink gediscussieerd met de stakeholders en uiteindelijk is besloten om punt 2 op te pakken. Dit besluit is genomen omdat hiermee in een keer alle accountants vanuit de business door deze nieuwe BI-Tooling ontlast worden en het gebruik van dit nieuwe hulpmiddel in één keer breed wordt gecommuniceerd met de reguliere bedrijfsvoering. In de toekomst wordt het hierdoor eenvoudiger om nieuwe onderdelen toe te voegen en deze uit te rollen in de organisatie. Concreet betekent dit dat de BI-Tooling door de accountants in het kader van de jaarrekeningcontrole gebruikt zal worden om per fase vast te stellen of aan alle Nederlandse wet- en regelgeving in het kader van de jaarrekeningcontrole wordt voldaan.

3. Kwaliteit van data
Om de datakwaliteit te kunnen garanderen worden alleen basisvelden, waarvan de juistheid reeds is vastgesteld, vanuit het auditdossier overgenomen. In de eerste versie van de BI-Tool worden deze basisvelden via een SFTP-server overzet van het auditdossier naar de BI-Tool.

4. Omvang BI-ontwikkelproject
Bij succesfactor 2 is reeds aangegeven dat de BI-Tooling ontwikkeld zal worden om per controledossier vast te stellen of aan alle Nederlandse wet- en regelgeving wordt voldaan. Het ontwikkeltraject moet in drie maanden afgerond worden vóór 1 juni 2018. Hiermee zijn de omvang en de tijdsbesteding voor het ontwikkeltraject concreet geformuleerd.

5. Segmentatie van oplossingen voor individuele gebruikersgroepen
Bij deze eerste ontwikkeling van een BI-Tooling in het kader van de jaarrekeningcontrole is ervoor gekozen om deze niet te segmenteren voor de individuele gebruikersgroepen. Voor de langere termijn is het waardevol om de oplossingen specifiek te maken voor de verschillende gebruikersgroepen. Uit de afstemming met de stakeholders blijkt ook dat dit geen belangrijk aandachtspunt is voor de ontwikkeling van de eerste BI-Tooling.

6. Projectsponsor
Alle stakeholders vonden het hebben van een projectsponsor belangrijk voor het slagen van het project. Zij gaven aan dat vooral de link tussen mijn ontwikkelteam en de eindverantwoordelijke belangrijk was. De projectsponsor gezorgd ook voor communicatie met de andere stakeholders waaronder de directieleden en de raad van toezicht. De projectsponsor heeft mij ook gecoacht met operationele aangelegenheid zoals het nemen van de juiste beslissingen tijdens het prioriteren van de diverse ontwikkelactiviteiten.

7. Ondersteuning vanuit topmanagement

Door het belang van deze ontwikkeling heb ik in overleg met het stakeholder A besproken hoe topmanagement betrokken kan worden bij de ontwikkeling van deze BI-Tooling. Topmanagement was vertegenwoordig als een stakeholder. Daarnaast is een inspiratiesessie gegeven een afvaardiging om de support te verkrijgen, hetgeen ook gebeurd is. Om zichtbaar te ondersteunen heeft een afvaardiging input geleverd tijdens de testfases. Hiermee kon aangetoond worden dat keuzes gedurende het proces ook zijn voorgelegd aan topmanagement. Tevens is dit aan een deel van het bestuur gepresenteerd en zij hebben goedkeuring gegeven om deze innovatie door te zetten. Op deze manier is 'buy-in' vanuit topmanagement verkregen.

8. Adequaat team met softwareontwikkelaars
De stakeholders die primair verantwoordelijk waren voor de uitvoering van de softwareontwikkeling gaven aan dat dit een belangrijke succesfactor is. Het team diende te bestaan uit teamleden die zich konden committeren aan de visie en primaire doelstellingen voor de ontwikkeling van deze eerste BI-Tooling. Doordat een core-team gevormd was vanuit de verschillende disciplines bezat het team de juist technische en functionele vaardigheden. Het gezamenlijke doel was helder en betekenisvol waardoor de collega's eigenaarschap namen voor de taken die zij toebedeeld kregen.

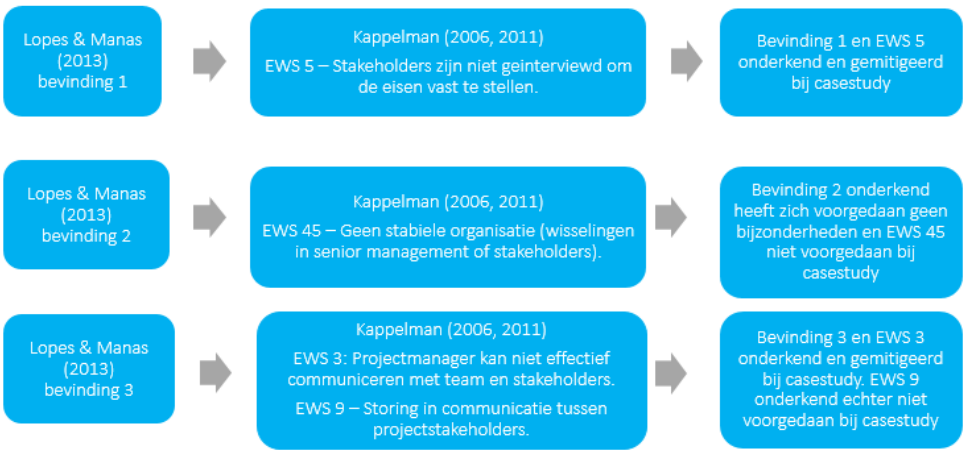
9. Continue ondersteuning
Het geven van continue ondersteuning werd door de stakeholders die verantwoordelijk zijn voor de content opgenomen als belangrijke succesfactor. Om dit te realiseren heb ik een wekelijks overleg gepland om de status van de afgelopen iteratie en de komende iteratie te bespreken.

10. Open bedrijfscultuur
Om te komen tot een BI-Tooling die direct effectief is en die ook nog efficiënt ontwikkeld is moet de organisatie voldoende aandacht geven aan dit project. De voorgaande succesfactoren hebben een stevige basis gelegd maar een open (bedrijfs)cultuur bij de ontwikkeling is cruciaal. Het delen van kennis, ervaring, obstakels en imperfecties gedurende de iteraties past binnen een open cultuur die aanwezig was tijdens het ontwikkeltraject.

3.3.2 Toetsing van de verschillende modellen

Gedurende het ontwikkelproces zijn de best practices en de overige modellen uit het theoretisch kader getoetst aan de praktijk. De risico's worden afgedekt door de succesfactoren, maar ze zorgen niet altijd voor de beschreven effecten vanuit de theorie. Daarnaast zijn aanvullende maatregelen genomen om nieuwe en/of bestaande risico's te mitigeren met als doel de BI-Tooling in te zetten bij de jaarrekeningcontrole.
In de beginfase van het ontwikkelproces werd mij duidelijk dat de collega's uit de auditpraktijk de uiteindelijke gebruikers waren voor wie deze BI-Tooling werd gemaakt. Doordat het eindproduct werd gemaakt voor deze groep miste ik een vertegenwoordiger van hen als stakeholder. Om deze input toch te krijgen heb ik als projectleider een klankbordgroep opgericht bestaande uit een representatieve groep collega's uit de auditpraktijk. Gedurende het verdere ontwikkelproces heeft het ontwikkelteam bij de verschillende iteraties afstemming met deze relevante eindgebruikers gehad. De toevoeging van deze belangrijke stakeholder was een toevoeging ten opzichte van de projectopzet. Door Lopes & Manas (2013) is deze nieuwe toevoeging gedurende het ontwikkeltraject benoemd als vertragingsrisico. Bij het praktijkonderzoek heeft dit niet gezorgd voor vertraging, maar eerder voor een versnelling omdat bevestiging vanuit de eindgebruikers zorgde voor snellere besluitvorming. Dit ging met name sneller doordat discussies met de content owners minder tijd kostten doordat discussiepunten voorgelegd konden worden aan de eindgebruikers. De validatie door de eindgebruikers sluit aan bij een Agile-werkmethode. Hiermee zijn twee van de drie specifieke gebreken bij stakeholdermanagement geadresseerd die door Lopes & Manas (2013) werden onderkend. Het laatste betreft slechte communicatie tussen IT-projectmanagement en stakeholders door het

ontbreken van een gezamenlijk doel. Bij deze ontwikkeling is dit gezamenlijke doel middels de roadmap als onderdeel één het model van Mesaros.
In het theoretisch kader zijn de gebreken binnen stakeholdermanagement van Lopes & Manas (2013) gekoppeld met de EWS van Kappelman (2006, 2011). De drie gebreken en de bijhorende EWS zijn opgevolgd. De punten van Lopes & Manas zijn reeds in de voorgaande alinea behandeld. De stakeholders zijn geïnterviewd om de eisen vast te stellen waarmee EWS 5 is gemitigeerd. De organisatie is stabiel en de toevoeging van één stakeholder heeft niet geleid tot verstoringen. Hierdoor heeft EWS 45 zich niet voorgedaan. Om de effectiviteit van de communicatie tussen projectmanager, het team en de stakeholder te vergroten zijn wekelijkse bijeenkomsten gepland als onderdeel van het model van Mesaros 'Continue ondersteuning'. Hierdoor was er voldoende ruimte voor onderlinge afstemming en kon ruggespraak met de stakeholders plaatsvinden; hiermee is EWS 3 gemitigeerd. Storingen in de communicatie tussen de projectstakeholders hebben niet plaatsgevonden doordat deze nauw betrokken waren en conform de opzet regelmatig werden geüpdatet over het proces. Doordat dit een innovatie betrof heeft het ontwikkelteam tevens uitleg gegeven over de technische ontwikkeling zoals de gedefinieerde business rules. Hierdoor was er geen indicatie voor EWS 9 tijdens het ontwikkelproces.



(Figuur 10 Uitkomst Lopes versus Kappelman tijdens casestudy – eigen ontwerp)

De ontwikkeling van de BI-Tooling binnen het SOFY-platform heeft plaatsgevonden op basis van de Agile werkmethode en de onderkende succesfactoren vanuit het theoretisch kader zijn grotendeels gehanteerd bij de uitvoering. Hieronder is als volgt weergegeven of Agile werken in combinatie met de succesfactoren gehanteerd is: + = toegepast, +/- gedeeltelijk toegepast en -/- niet toegepast. Daarna worden de uitzonderingen +/- gedeeltelijk toegepast en -/- niet toegepast toegelicht.

Onderdeel Agile proces	Principes (Dyba et al) ten behoeve van succes	Toetsingselementen (Trijssenaar en Zalm) succesvolle toepassing	Implementatie binnen casestudy
Agile-ontwikkel-documentatie	Minimale zwaarwegende specificaties	Verzamelde eisen en wensen in use cases, vaststellen aanwezigheid, accordering en format	+
		Burndown chart, aanwezigheid en weergave actuele standen	+/-
Werking Agile-proces	Continu leren door middel van feedback	Planning van de iteraties overleggen	+
		Backlogs iteraties	+
		Retrospectief deel van sprint overleg	+
Rand-voorwaarden team in Agile-proces	Autonome teams inclusief redundantie in teams	Vertegenwoordiging senior staff zijnde product owner van de BI-Tooling	+
		Team samenstelling kennis en ervaring	+/-
		Communicatie tussen Agile team en product owner	+
Inzet middelen ten behoeve van project	Combinatie minimale zwaarwegende specificaties en autonomen teams	Geleverde functionaliteiten in timeboxen	+/-
		Geleverde functionaliteiten met aantal mensuren ter indicatie van kwaliteit	-

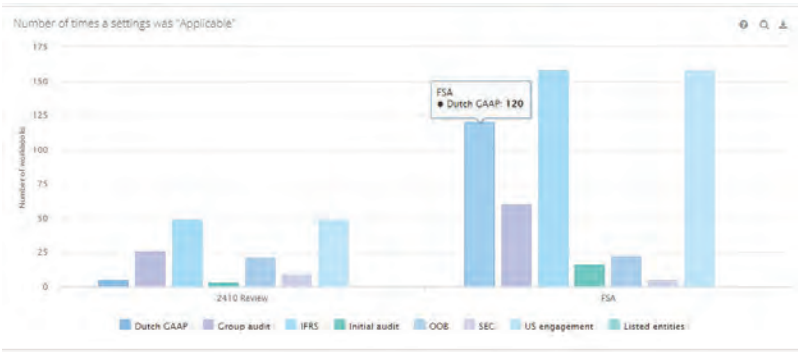
(Figuur 11 Uitkomst Agile versus Dyba et al. tijdens casestudy – eigen ontwerp)

De eerste uitzondering ten opzichte van de toetsingselementen om succesvolle toepassing van Agile te realiseren en te toetsen is 'Burndown chart, aanwezigheid en weergave actuele standen'. Dit is deels toegepast: burndown charts actualiseren hiervoor was onvoldoende tijd en er waren geen andere resources beschikbaar waaraan dit uitbesteed kon worden. De tweede uitzondering betreft 'Teamsamenstelling, kennis en ervaring'. Het team was adequaat opgebouwd ; een aantal vaardigheden werden echter gedurende het project opgedaan. Dit betrof het verkrijgen van kennis van de BI-Tooling door de uitvoerende teamleden en het opdoen van ervaringen met Agile werken.
Om de kwaliteit van de softwareontwikkeling te maximaliseren is gekozen voor een gestructureerde aanpak op basis van PRINCE2 in combinatie met de Agile werkmethode. In de BI-Tooling wordt de gebruiker gefaciliteerd door verschillende datastromen. Deze data-elementen hebben verschillende datatypen. Om ervoor te zorgen dat de datakwaliteit tijdens het gebruik van de BI-Tooling van hoog niveau blijft, zijn er door de accountantsorganisatie een aantal mitigerende controlemaatregelen genomen. Door de gestructureerde aanpak conform PRINCE2 heeft het implementeren van deze mitigerende maatregelen efficiënt kunnen plaatsvinden.
In hoofdstuk 2 paragraaf 2.2.4 is reeds het kader met de verschillende elementen van de gestructureerde aanpak op basis van PRINCE2 in combinatie met de Agile werkmethode uitgewerkt. De uitvoering volgens de gestructureerde aanpak heeft plaatsgevonden conform de theorie met uitzondering van de volgende drie bijzonderheden.

Projectfase	PRINCE2 Hoofdproces(sen)	PRINCE2 Thema(s)	Onderdeel Agile proces	Onderdeel Agile proces
Voorbereiden en starten ontwikkelproject	Initiëren van het project	Plannen, kwaliteit, risico, businesscase.	Agile-ontwikkeldocumentatie	Iteratie(s)
Uitvoering ontwikkelproject	Managen van opleveren ontwikkel-producten	Wijziging, kwaliteit, voortgang	Werking Agileproces	Iteratie(s)
Afsluiting ontwikkelproject	Formeel sluiten van het ontwikkelproject	Kwaliteit, Businesscase	BI-Tooling is in productie en monitoren gebruik incl. start versie 2	Einde van alle iteraties in sprint

(Figuur 12 Uitkomst PRINCE2 gekoppeld met Agile tijdens de casestudy – eigen ontwerp)

Ten eerste was tijdens de voorbereiding het opnemen van de eisen ten aanzien van het thema kwaliteit en de risico's in de verdere Agile ontwikkeldocumentatie niet eenvoudig. Door de gangbare werkmethodes ontstond al snel een waslijst aan kwaliteitseisen, mogelijke risico's en overige bezwaren. In eerste instantie zijn deze geparkeerd om een werkend PoC te kunnen tonen. Hiermee was een deel van de waslijst al opgelost. Het adresseren en het prioriteren van de resterende items heeft veel tijd gekost. Hiermee kom ik ook direct bij het tweede punt: het werken in iteraties zat niet direct in het DNA van het ontwikkelteam. Het opdoen van praktijkervaring zorgde wel voor een steile leercurve. Het omgaan met wijzigingen, het waarborgen van de kwaliteit en het gelijktijdig managen van de voortgang kostten meer tijd dan bij de start was voorzien. Het derde en laatste punt betreft het afsluiten van het ontwikkelproject; door de vertraging eerder in het traject was het op het einde nodig om meer tijd te nemen voordat de BI-Tooling ingezet kon worden. Hiervoor is in overleg met de stakeholders gekozen het ontwikkelproject met twee sprints te verlenen zodat voldoende tijd was om aanvullende kwaliteitscheck uit te voeren.
Voorafgaande waren een aantal KPI's geformuleerd welke ontleend konden worden aan de data in de BI-Tooling. Hieronder is ter illustratie een deel van het KPI-dashboard opgenomen waarin testdata is weergegeven.



(Figuur 13 Uitkomst KPI-dashboard tijdens de casestudy – eigen ontwerp)

4 Analyse en conclusies

In dit hoofdstuk is in aanvulling op hoofdstuk 3 de analyse van de casestudy weergegeven in paragraaf 4.1. Daarna zijn de belangrijkste beperkingen van dit onderzoek, inclusief mogelijke kansen voor vervolgonderzoek, weergegeven in paragraaf 4.2. Tot slot wordt de tweede deelvraag 'Welke mitigerende controlemaatregelen worden in de praktijk genomen door de accountantsorganisatie met betrekking tot risico's bij de inzet van BI-Tooling met betrekking tot opzet, bestaan en werking?' beantwoord in paragraaf 4.3.

4.1 Analyse

Tijdens het uitvoeren van het praktijkonderzoek hebben de stakeholders ervaren dat het lastig is om ervoor te zorgen dat de BI-Tooling in overeenstemming is met andere verplichtingen van de organisatie. Gedurende het praktijkonderzoek is door het ontwikkelteam nauw samengewerkt met bureau vaktechniek en de risk department. Hierbij hebben de betrokkenen geleerd dat het bereiken van consensus over de content cruciaal is alvorens deze wordt ingeprogrammeerd in de BI-Tooling. De uiteindelijke tool voert de taak uit conform de meegegeven condities. Als deze condities onjuist zijn, werkt de tooling juist maar is de gebruiker ontevreden. Door een adequaat testpanel heeft het ontwikkelteam de meeste van deze obstakels kunnen corrigeren voor de livegang van de tool. Ik beveel andere ontwikkelaars aan om voor dit punt vooraf voldoende tijd in te calculeren. Bij dit praktijkonderzoek was het een van de belangrijkste oorzaken van het verschuiven van de initiële streefdatum van de livegang. Overall mis ik vanuit de succesfactoren prioritering; binnen de gehele ontwikkeling vanuit de verschillende modellen worden hiervoor geen handvatten geboden.

Wat daarnaast opviel was dat in eerste instantie van te veel data de datakwaliteit is getest. Dit werd veroorzaakt doordat gedurende het proces is besloten om de datastroom vanuit het controledossier naar de BI-Tooling te reduceren. De vooraf bedachte aanpak is tijdens de verschillende iteraties bijgesteld om een beter eindproduct te realiseren. Het later in het proces testen van de datakwaliteit was efficiënter geweest. Voor verdere ontwikkeling zou ik willen aanraden om vooraf vast te stellen welke data minimaal verkregen moet worden. Die data kan tussentijds getest worden, voor overige data zou ik later in het proces deze taak opnemen in een iteratie. Dit is vooral een attentiepunt om te zorgen voor een efficiënt softwareontwikkelproces.

In de basis is Agile gewerkt door de BI-Tooling stapsgewijs met een iteratief proces te ontwikkelen. Er is alleen nooit een duidelijke keuze gemaakt welke specifieke methodiek gehanteerd zou worden, bijvoorbeeld XP (Extreme Programming), Feature-Driven Development (FDD), KANBAN, RUP (Rational Unified Process) of Scrum. Tevens zijn de stakeholders niet aanvullend getraind in deze werkmethode. Dit is een mogelijke oorzaak voor het gedeeltelijk toepassen en niet toepassen van de principes van Dyba et al. en de toetsingselementen voor succesvolle toepassing van Agile door Trijssenaar & Zalm zoals weergegeven in figuur 18.

4.2 Beperkingen van het onderzoek

PoC voor de onderwijsinstelling zoals weergegeven in hoofdstuk 1 is geslaagd en uitrol van de BI-Tooling binnen de gehele Nederlandse controlepraktijk heeft direct plaatsgevonden. De ontwikkeling van deze BI-Tooling wordt als zeer succesvol beoordeeld. Als reflectie op de gehele ontwikkeling is opgevallen dat de modellen voor succesvolle BI-ontwikkeling geen prioritering in model hebben opgenomen. In de dagelijkse praktijk moeten vaak keuzes gemaakt worden om te bepalen wat wel of niet gedaan wordt in een iteratie. Door vertraging in de content is de eerste opleverdatum van 1 juni uitgesteld naar in juni en dat tijdvak is breed gecommuniceerd binnen de organisatie. Het is vanuit de modellen en de resultaten uit de casestudy onbekend welke effecten dit heeft gehad op het eindresultaat. Vervolgonderzoek zou hier duidelijkheid over kunnen verschaffen, bijvoorbeeld middels een simulatieonderzoek.

De KPI's die gegenereerd konden worden aan de hand van de data in de BI-Tooling hebben door visualisatie meer inzicht gegeven dan vooraf was gedacht. Middels drill-downs konden specifieke opdrachten geselecteerd worden vanuit de algemene KPI-rapportage. Deze nieuwe inzichten worden als zeer waardevol ervaren. Het verkrijgen van deze actuele inzichten heeft bijgedragen aan het succes van deze ontwikkeling. Het bepalen van een succesvolle ontwikkeling hangt ook af van de perceptie. De stakeholders zijn zeer tevreden met de werkende BI-Tooling, maar hebben beperkt inzicht in de technische robuustheid en toekomstbestendigheid van de ontwikkelde applicatie.
Gedurende de ontwikkelfase van het praktijkonderzoek was het testen van de datakwaliteit die meegenomen werd in de BI-Tooling zeer relevant aangezien betrouwbare data de basis vormt van de verdere tool. In eerste instantie werd een omvangrijke datastroom overgenomen uit het controledossier. Tijdens de ontwikkeling is deze stroom in overleg met de stakeholder vanuit bureau vaktechniek gereduceerd door de vraagstellingen te wijzigen. Voor de resterende data is met een aantal query's de kwaliteitstoets van de data bepaald en deze is toereikend geacht. Als bij een ontwikkeling wel alle eerder verkregen data gebruikt moet worden, dan dienen intensievere kwaliteitscontroles uitgevoerd te worden en dienen eventuele herstelwerkzaamheden uitgevoerd te worden. Binnen dit onderzoek zijn hierover beperkte inzichten verkregen; hieraan kunnen derhalve ook geen verdere conclusies worden verbonden. Bij een vervolgonderzoek zou dit specifieke element expliciet onderzocht kunnen worden.

4.3 Beantwoording tweede deelvraag

Als sluitstuk van de casestudy in hoofdstuk 3 en bijbehorende analyse in dit hoofdstuk wordt de tweede deelvraag beantwoord. De tweede deelvraag 'Welke mitigerende controlemaatregelen worden in de praktijk genomen door de accountantsorganisatie met betrekking tot risico's bij de inzet van BI-Tooling met betrekking tot opzet, bestaan en werking?' kan op basis van de voorgaande paragrafen beantwoord worden. Het organiseren van de ontwikkeling van de BI-Tooling is een van de belangrijkste maatregelen om risico's voor de inzet van de BI-Tooling te mitigeren. Het hoofdmodel van Mesaros in combinatie met de overige modellen hebben geleid tot een succesvolle ontwikkeling. De technische en projectmatige risico's zijn in opzet onderkend bij aanvang van het project. Vervolgens zijn mitigerende (controle)maatregelen genomen om deze risico's af te dekken zodat de BI-Tooling een adequaat hulpmiddel is dat ingezet kan worden bij de jaarrekeningcontrole.

5 Aanbevelingen theorie en praktijk

5.1 Inleiding

In het kader van deze publicatie wordt in dit hoofdstuk een verkorte versie van de verbeterpunten en attentiepunten weergegeven die tijdens het onderzoek zijn geïdentificeerd. In het verlengde daarvan worden aanbevelingen gedaan. Hierbij is gezocht naar mogelijke verklaringen en is aangegeven in welke richting vervolgonderzoek uitkomsten kan bieden. Hiermee wordt op basis van de casestudy de derde deelvraag 'Welke verbeterpunten en/of attentiepunten zijn geïdentificeerd gedurende de eerste implementatie van de BI-Tooling voor de jaarrekeningcontrole en welke aanbevelingen kunnen worden gegeven?' beantwoord.

5.2 Verbeter- en/of attentiepunten

Het literatuuronderzoek was opgezet om een theoretisch kader op te bouwen om ervoor te zorgen dat de te ontwikkelen BI-Tooling ingezet kon worden bij jaarrekeningcontroles. Met focus op de risico's en de beperkingen vanuit wet- en regelgeving. Bij het uitwerken van het literatuuronderzoek kwam ik tot de conclusie dat de risico's met name gericht zijn op de softwareontwikkeling en dat er vanuit wet- en regelgeving geen noemenswaardige beperkingen zijn. Vervolgens zijn een aantal modellen gevonden die konden bijdragen aan het mitigeren van de risico's. Het belangrijkste model betrof het model van Mesaros waarin is aangegeven welke kritieke succesfactoren overwogen moeten worden om tot een succesvolle

ontwikkeling en implementatie te komen. Bij alle ontwikkelingen dient rekening gehouden te worden met wet- en regelgeving en met het toevoegen van additionele vereisten naar aanleiding van wijzigingen in wet- en regelgeving.
De uitkomsten van dit praktijkonderzoek hebben aangetoond dat het model van toegevoegde waarde is bij het ontwikkelen van BI-Tooling. Het toepassen van een minder algemeen bekend model heeft voor nieuwe invalshoeken gezorgd welke cruciaal zijn bij innovatieve softwareontwikkeling. Een model met gevestigde toetsingsnormen zoals: ISO-normen, COBIT, ITIL was zeker passend geweest maar ik ben van mening dat die minder hadden bijgedragen aan het innovatieve karakter van deze ontwikkeling. Een dergelijk model had kunnen bijdragen aan de innovatie, maar het had ook gehanteerd kunnen worden als de zoveelste checklist. Het Mesaros-model is gevalideerd door het praktijkonderzoek waarmee toepassing van dit model passend wordt geacht bij verdere ontwikkelingen in de praktijk en heeft daarmee de bestaande literatuur verrijkt. Als attentiepunt wordt meegegeven om bij volgende ontwikkelingen vast te stellen of dit model passend is gezien de situatie.
Ten slotte, er bestaat nog geen passend volwassenheidsmodel waaraan BI-Tooling die ontwikkeld wordt getoetst kan worden. Om diverse stakeholders te overtuigen bij de implementatie van BI-Tooling zou een toetsing die periodiek kan plaatsvinden voor meer vertrouwen kunnen zorgen. In de afrondende fase van het ontwikkeltraject ben ik wel Gartner's ITScore for Business Intelligence and Analytics uit 2015 tegengekomen. Hierin wordt meer de bereidwilligheid binnen de organisatie ten aanzien van implementatie van BI-Tooling bepaald om bij te kunnen dragen aan de bredere bedrijfsdoelstellingen. Vanuit de succesfactoren en het model van Mesaros wordt al sterk aanbevolen om de elementen toe te voegen die passen bij de hoogste levels van het model van Gartner. Retrospectief is het interessant om te zien dat hier sprake is van overlap en verder literatuuronderzoek had mogelijk andere inzichten gegeven.

5.3 Aanbevelingen

Algemene IT-auditnormen zijn vaak gericht op informatiebeveiliging, interne beheersing, bescherming van gegevens en/of de volwassenheid van het informatiesysteem. Voor de BI-Tooling zijn deze afzonderlijke aspecten in het kader van dit onderzoek niet separaat getoetst. Voordat deze BI-Tooling is geïmplementeerd bij een groot accountantskantoor heeft validatie van de tool door diverse afdelingen plaatsgevonden, waarbij algemene IT-auditnormen regelmatig als basis worden gehanteerd. Voor toetsing door een IT-auditor bij een externe organisatie beveel ik sterk aan om een aantal van deze algemene IT-auditnormen ook te toetsen of deze uitdrukkelijk buiten het onderzoek te laten. Echter, bepaalde minimale toetsingen zullen mijns inziens toch moeten plaatsvinden in het kader van data privacy.
Gedurende de ontwikkelfase van het praktijkonderzoek konden de content owners zorgen voor testers uit de eigen formatie. Het eindproduct werd gemaakt voor de auditpraktijk: zij zijn de uiteindelijke gebruikers. Derhalve zijn zij als testers een representatievere groep. Ik merkte vooral dat de testers vanuit de praktijk in eerste instantie meer kijken naar gebruiksgemak en minder naar of de BI-Tooling de juiste stappen. Tijdens de tweede testfase ontstaan ook content gerelateerde vragen en verzoeken om verbetering in de tool. Mijn aanbeveling voor toekomstige ontwikkeling is om de content ook eerst te laten beoordelen door testers uit de dagelijkse praktijk. Hiermee kunnen onduidelijkheden en verzoeken om additionele toelichting eerder geadresseerd worden. Hierdoor wordt het risico op een langere ontwikkelperiode voorkomen.

5.4 Beantwoording derde deelvraag

Als sluitstuk van de analyse wordt de derde deelvraag beantwoord. De derde deelvraag 'Welke verbeterpunten en/of attentiepunten zijn geïdentificeerd gedurende de eerste implementatie van de BI-Tooling voor de jaarrekeningcontrole en welke aanbevelingen kunnen worden gegeven?' kan op basis van de adviezen in de voorgaande paragraaf beantwoord worden. De belangrijkste vier adviezen die bestaan uit verbeterpunten en attentiepunten zijn:

1 Het Mesaros-model is gevalideerd door het praktijkonderzoek en kan ingezet worden bij volgende ontwikkelingen. In aanvulling hierop dient bij alle ontwikkelingen rekening gehouden te worden met

wet- en regelgeving en met het toevoegen van additionele vereisten naar aanleiding van wijzigingen in wet- en regelgeving. Als attentiepunt wordt meegegeven om bij volgende ontwikkelingen vast te stellen of dit model passend is gezien de situatie.

2 De Agile werkmethode is geïdentificeerd als een succesfactor; als attentiepunt wordt opgemerkt dat ervoor gezorgd dient te worden dat alle betrokkenen voorafgaand getraind zijn in de basisprincipes van de te hanteren werkmethode.

3 Bij toepassing van de modellen om succesvol te ontwikkelen ontbreekt prioritering. Dit zou toegevoegd kunnen worden aan een van de modellen na verder onderzoek of aanvullend kunnen worden toegevoegd in de verschillende fases van de ontwikkeling. Deze aanbeveling dient gezien te worden als een verbeterpunt.

4 Om het digitaliseringsproces succesvol te maken is het belangrijk om eerst de content te beoordelen die gedigitaliseerd gaat worden. Dit dient gedaan worden door experts op het gebied van de content in samenspraak met medewerkers uit de dagelijkse praktijk. Hiermee kunnen onduidelijkheden en verzoeken om additionele toelichting eerder geadresseerd worden. Vervolgens moet de content gefixeerd worden zodat tijdens de ontwikkeling geen verstoringen door het wijzigen van content optreden.

6 Beantwoording onderzoeksvraag (conclusie)

In dit hoofdstuk worden de conclusies van dit onderzoek weergegeven. De weergave is uitgesplitst in de drie deelvragen in paragraaf 6.1. De vraagstelling is behandeld in paragraaf 6.2. van dit hoofdstuk waarmee de onderzoeksvraag wordt beantwoord.

6.1 Conclusie deelvragen

Uit het literatuuronderzoek komt een verrassende uitkomst waaruit blijkt dat innovatieve IT-hulpmiddelen het proces van de jaarrekeningcontrole kunnen verrijken. De eerste deelvraag die is beantwoord middels het theoretisch kader luidt als volgt:

1 *Aan welke voorschriften en richtlijnen moet voldaan worden om verkregen inzicht vanuit een BI-Tooling te kunnen gebruiken in het kader van de jaarrekeningcontrole en welke risico's zijn hierbij te onderscheiden?*

Formeel gezien zijn er vanuit wet- en regelgeving geen beperkingen om BI-Tooling in te zetten. De BI-Tooling kan als ondersteunend hulpmiddel worden ingezet bij de jaarrekeningcontrole. Het succesvol ontwikkelen van BI-Tooling kan significant bijdragen aan de kwaliteit van jaarrekeningcontroles. Om dit te realiseren zijn technische en projectmatige risico's onderkend. Om deze succesvol te adresseren zijn diverse modellen ontwikkeld. De projectmatige en beproefde basis van PRINCE2, de succesfactoren van het model van Mesaros en een iteratieve ontwikkelmethode van Agile zorgen gecombineerd voor een robuustere softwareontwikkeling. Op basis van het literatuuronderzoek zijn deze passende modellen gecombineerd om een succesvolle ontwikkeling te realiseren.

De tweede deelvraag die beantwoord kan worden vanuit de resultaten van de casestudy luidt als volgt:

2 *Welke mitigerende controlemaatregelen worden in de praktijk genomen door de accountantsorganisatie met betrekking tot risico's bij de inzet van BI-Tooling met betrekking tot opzet, bestaan en werking?*

Het organiseren van de ontwikkeling van de BI-Tooling is een van de belangrijkste maatregelen om risico's voor de inzet van de BI-Tooling te mitigeren. Het hoofdmodel van Mesaros in combinatie met de overige modellen heeft geleid tot een succesvolle ontwikkeling. De technische en projectmatige risico's zijn in opzet onderkend bij aanvang van het project. Vervolgens zijn mitigerende (controle)maatregelen genomen om deze risico's af te dekken zodat de BI-Tooling een adequaat hulpmiddel dat ingezet kan worden bij de jaarrekeningcontrole.

De derde deelvraag betreft een beschouwende deelvraag waarbij aanbevelingen zijn geformuleerd op basis van de inzichten die zijn verkregen tijdens het uitvoeren van de casestudy. Deze deelvraag luidt als volgt:

3 Welke verbeterpunten en/of attentiepunten zijn geïdentificeerd gedurende de eerste implementatie van de BI-Tooling voor de jaarrekeningcontrole en welke aanbevelingen kunnen worden gegeven?

De belangrijkste vier adviezen die bestaan uit verbeterpunten en attentiepunten zijn:

1 Het Mesaros-model is gevalideerd door het praktijkonderzoek en kan ingezet worden bij volgende ontwikkelingen. In aanvulling hierop dient bij alle ontwikkelingen rekening gehouden te worden met wet- en regelgeving en met het toevoegen van additionele vereisten naar aanleiding van wijzigingen in wet- en regelgeving. Als attentiepunt wordt meegegeven om bij volgende ontwikkelingen vast te stellen of dit model passend is gezien de situatie.
2 De Agile werkmethode is geïdentificeerd als een succesfactor; als attentiepunt wordt opgemerkt dat ervoor gezorgd dient te worden dat alle betrokkenen voorafgaand getraind zijn in de basisprincipes van de te hanteren werkmethode.
3 Bij toepassing van de modellen om succesvol te ontwikkelen ontbreekt prioritering. Dit zou toegevoegd kunnen worden aan een van de modellen na verder onderzoek of aanvullend kunnen worden toegevoegd in de verschillende fases van de ontwikkeling. Deze aanbeveling dient gezien te worden als een verbeterpunt.
4 Om het digitaliseringsproces succesvol te maken is het belangrijk om eerst de content te beoordelen die gedigitaliseerd gaat worden. Dit dient gedaan worden door experts op het gebied van de content in samenspraak met medewerkers uit de dagelijkse praktijk. Hiermee kunnen onduidelijkheden en verzoeken om additionele toelichting eerder geadresseerd worden. Vervolgens moet de content gefixeerd worden zodat tijdens de ontwikkeling geen verstoringen door het wijzigen van content optreden.

6.2 Conclusie vraagstelling

Op welke wijze en in hoeverre heeft het inzetten van Business Intelligence door middel van (deels) geautomatiseerde tooling binnen de controlefase van jaarrekeningcontroles toegevoegde waarde?

Wet- en regelgeving staat verdere automatisering en het inzetten van bijvoorbeeld BI-Tooling toe. Het verbeteren van de werkstroom door bijvoorbeeld een aantal voorloopvragen en vervolgens per onderwerp diverse vervolgvragen geeft een (deels) geautomatiseerde beslisboom. Deze structuur zorgt voor focus wat leidt tot efficiency. Door de focus kan onder andere meer tijd besteed worden aan de relevante onderwerpen. De toegevoegde waarde heeft betrekking op drie dimensies: kwaliteit, het verstrekken van (nieuwe) inzichten en het verbeteren van de werkstroom. Als geautomatiseerde tooling bij de uitvoering van jaarrekeningcontroles één van deze drie dimensies raakt, dan heeft dit al toegevoegde waarde. Gedurende de casestudy bleek de ontwikkelde BI-Tooling vooral bij te dragen aan het verbeteren van de werkstroom. De toegevoegde waarde hiervan was zo waardevol dat de BI-Tooling uitgerold is naar de hele Nederlandse controlepraktijk van de organisatie waar ik werkzaam ben. Hiermee draagt deze BI-Tooling bij aan het ontlasten van de gehele auditpraktijk waardoor dit van grote toegevoegde waarde is.

7 Literatuurlijst

7.1 Artikelen

Bi, L. (2009). Auditing IT projects. The Journal of Corporate Accounting & Finance, 20(5), 55-57.
Brooks, Fred P. (1987). No silver bullet essence and accidents of software engineering. Computer, 20(4).
Cohen, E., Deal, T., Meyer, J., & Scott, W. (1979). Technology and Teaming in the Elementary School. Sociology of Education, 20-33.
Dyba, T. & Dingsoyr, T.(2015). Agile project management: from self-managing teams to large-scale development. ICSE '15: Proceedings of the 37th International Conference on Software Engineering - Volume 2, 945-946.
Eimers, P. & Amerongen, A. (2015), Ontwikkelingen in de toepassing van data-analyse voor de accountantscontrole. Maandblad voor Accountancy en Bedrijfseconomie, 346-347 89E jaargang oktober.
Horáková, M. & Skalsa, H., 2013: Business Intelligence and Implementation in a Small Enterprise. Journal of System Integration, Vol.4, Issue 2, pp. 50-61.
Kappelman, L. & Zhang, L. (2006). Early warning signs of IT project failure: The dominant dozen. Information Systems Management, 23(4), 31.
Kappelman, L. (2011). AUDITING IT Projects: early warning signs of material risk. Edpacs, 43(1), 1-9.
Lopes, L & Manas, A.V (2013). Delays in IT projects due to failures in the stakeholders management. Future Studies Research Journal: Trends and Strategies, 5(2), 155-186.
Mesaros, P., Carnicky, S., Mandicak, T., Habinakova, M., Mackova, D., & Spisakova, M. (2016). Model of key success factors for business intelligence implementation. Journal of Systems Integration, 3-15, 3-15.
Omoteso, K. (2014). Audit automation. Accountancy, (feb 2014).
Sommer, A.F. Hedegaard, C. Dukovska-Popovska, I & Steger-Jensen, K (2015) Improved Product Development Performance through Agile/Stage-Gate Hybrids: The Next-Generation Stage-Gate Process?, Research-Technology Management, 58:1, 34-45.
Trijssenaar, M. & Zalm, M. van der (2013) Agile-ontwikkelmethoden Auditen, de IT Auditor, nr. 3, pp. 10-14.

7.2 Boeken

King, M. & de Beer, L. (2018). The Auditor: Quo Vadis?, First Edition, Routledge.
Kranenburg, K. (2008). Software Factory, eerste druk, Academic Service, Den Haag, Nederland.
Reifer, D. (2002). Software management (6th ed. ed.). Los Alamitos, CA etc.: IEEE Computer Society Press.
Stutzke, R.D. (2005) Estimating Software-Intensive Systems: Projects, Products, and Processes (paperback), First Edition, Pearson Education (US).
Trendowicz, A. & Jeffery, R. (2014). Software project effort estimation : Foundations and best practice guidelines for success, First Edition, Springer.
Yin, R.K. (2008) Case Study Research, design and methods, Forth Edition, SAGE Publications Inc, London, United Kingdom.

7.3 Websites

Breij, W.A. & Havinga, H.B.P (2014,14 november). Informatie PRINCE2 alleen niet voldoende "Zachte factoren van business-IT alignment" geraadpleegd ten behoeve van criteria. [Geraadpleegd op 28 juli 2018, van https://www.deitauditor.nl/business-en-it/zachte-factoren-van-business-it-alignment/].
Cambridge University Press (2018). Toelichting van het begrip Tooling in Cambridge Dictionary [Geraadpleegd op 27 augustus 2018, van https://dictionary.cambridge.org/dictionary/english/tooling].
International Organization for Standardization (ISO) (2018). ISO Standaarden [Geraadpleegd op 6 juli 2018, van https://www.iso.org/ics/03.120.10/x/

ISACA (2018). Begrip business intelligence niet in woordenlijst ISACA [Geraadpleegd op 6 juli 2018, van https://www.isaca.org/Pages/Glossary.aspx?tid=1284&char=D].
Forrester (2018). Begrip business intelligence bij Forrester [Geraadpleegd op 6 juli 2018, van https://www.forrester.com/Business-Intelligence#].
Gartner (2017) Informatie met betrekking tot Analytics Platforms doorgenomen [Geraadpleegd op 2 januari 2018, van https://www.gartner.com/doc/3611117/magic-quadrant-business-intelligence-analytics]. Voor de lezers van deze scriptie: Gartner-inlog vereist om gehele artikel te kunnen lezen.
Gartner (2018). IT Woordenlijst business intelligence van Gartner [Geraadpleegd op 3 juli 2018, van https://www.gartner.com/it-glossary/business-intelligence-bi/].
Howson, C. Sallam, R.L. Richardson, J.L. Tapadinhas, J. Idoine, C.J. & Woodward, A. (2018). Informatie met betrekking tot top 20 Analytics Platforms uit artikel Magic Quadrant for Analytics and Business Intelligence Platforms. [Geraadpleegd op 19 juli 2018, van https://www.gartner.com/doc/3861464/magic-quadrant-analytics-business-intelligence]. Voor de lezers van deze scriptie: Gartner-inlog vereist om gehele artikel te kunnen lezen.

Keuningen, M.G. de Meijer, P.R. (2016). PRINCE2 bij projectmanagement “Projectmanagement, leren we het (n)ooit?” geraadpleegd ten behoeve van criteria [Geraadpleegd op 28 juli 2018, van https://www.compact.nl/articles/projectmanagement-leren-we-het-nooit/].
Koninklijke Nederlandse Beroepsorganisatie van Accountants (2018). Nadere voorschriften controle- en overige standaarden vastgesteld bij bestuursbesluit van 12 december 2017 onderdeel van het handboek richtlijnen accountants 2018 [Geraadpleegd op 6 juli 2018, van https://www.nba.nl/tools/hra-2018/?document=118817].
KPMG (2018, 2 januari). Informatie met betrekking tot volgende fase KPMG SOFY platform zijnde een Digital Risk Platform [Geraadpleegd op 2 januari 2018, van https://home.kpmg.com/nl/en/home/media/press-releases/2017/01/kpmg-launches-digital-risk-platform.html en op 25 september 2018 geraadpleegd in verband met re-branding nu bereikbaar via https://home.kpmg.com/nl/nl/home/services/advisory/technology/cyber-security-services/digital-risk-platform.html].
KPMG (2018-1). Toelichting toepassingsmogelijkheden KPMG SOFY BI Platform. [Geraadpleegd op 2 september 2018, van https://home.kpmg.com/nl/nl/home/services/advisory/technology/data-and-analytics/data-visualization-and-dashboarding.html].
KPMG (2018-2). Toelichting gebruikte technologie binnen KPMG SOFY. [Geraadpleegd op 2 september 2018, van https://www.kpmgsofy.com/platform/].
Maes, R (2017). Terugblik van Maes op zijn raamwerk voor informatiemanagement zijnde het negenvlak [Geraadpleegd op 2 september, van https://www.agconnect.nl/blog/het-amsterdams-negenvlak].
Moreh, J (2016). Illustratie Analytics weergegeven op titelpagina. [Geraadpleegd op 31 augustus 2018, van https://www.stockvault.net/photo/196879/big-data-analytics#].
De Nederlandse Orde van Register EDP-Auditors (NOREA) (2018). Regels en richtlijnen [Geraadpleegd op 6 juli 2018, van https://www.norea.nl/regels-en-richtlijnen].
Online van Dale (2018). Toelichting van het begrip Tool in de van Dale [Geraadpleegd op 27 augustus 2018, van https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/tool#.W4PkvMJlKUk].
PRINCE2 (2018). PRINCE2 geraadpleegd ten behoeve van criteria [Geraadpleegd op 28 juli 2018, van https://www.prince2.com/eur/prince2-methodology en https://www.prince2.com/eur/what-is-prince2#prince2-definition].
Schwartz, M. (2011). Begrip business intelligence uitgelegd bij ISACA event door Matt Schwartz 31 maart 2011 [Geraadpleegd op 6 juli 2018, van https://www.isaca.org/chapters1/phoenix/events/Documents/business_intelligence_overview.ppt].
TDWI (2018). Begrip business intelligence bij The Data Warehouse Institute [Geraadpleegd op 6 juli 2018, van https://tdwi.org/portals/what-is-self-service-bi-and-analytics-definition.aspx].

Waa, F van der & Griffioen, T.D. (2013). Informatie met betrekking ‘A structured approach to improving business intelligence’ artikel in Compact [Geraadpleegd op 31 januari 2018, van https://www.compact.nl/articles/a-structured-approach-to-improving-business-intelligence/?zoom_highlight=Business+Intelligence].

Privacy by Design

Hilde van Dijk
Ajay Bisnajak

Ajay Bisnajak en Hilde van Dijk hebben een goede samenwerking gehad tijdens de IT-Audit opleiding aan de VU. Dit resulteerde uiteindelijk in een gezamenlijk afstudeerproject 'Privacy by Design – realisatie en compliance bij informatie-intensieve organisaties'. Deze scriptie werd afgerond in april 2018, een maand voordat de General Data Protection Regulation (GDPR) of - in het Nederlands - de Algemene Verordening Gegevensbescherming (AVG) van toepassing werd. Ajay werkt als auditor bij de Rabobank en Hilde werkt als auditor bij de Sociale Verzekeringsbank. Beiden hebben sinds het afstuderen de opgedane kennis in de praktijk kunnen brengen in de uitvoering van audits met betrekking tot de implementatie van de nieuwe wetgeving.

1 Inleiding

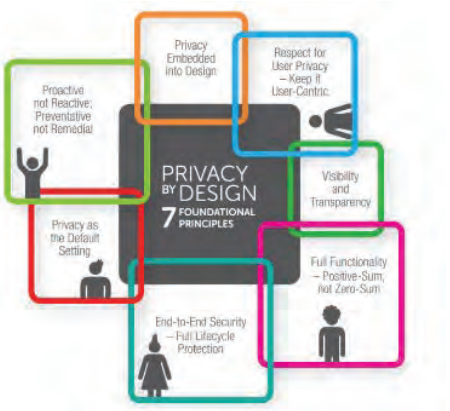
Op 25 mei 2018 is de General Data Protection Regulation (GDPR) of - in het Nederlands - de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De AVG volgt op deze datum de Richtlijn 95/46/EG van het Europees Parlement en de van deze Europese richtlijn afgeleide Nederlandse Wet bescherming persoonsgegeven (Wbp) op. Onderdeel van de AVG is artikel 25 over gegevensbescherming door ontwerp en door standaardinstellingen. Dit onderwerp is beter bekend als Privacy by Design en Privacy by Default.

De tekst van AVG artikel 25 komt inhoudelijk grotendeels overeen met de tekst van Wbp artikel 13. Zowel AVG artikel 25 als Wbp artikel 13 spreken in het kader van bescherming van persoonsgegevens van passende technische en organisatorische maatregelen, van het rekening houden met de stand der techniek, met de kosten van de tenuitvoerlegging en met de aan de verwerking verbonden risico's. In de AVG wordt niet zoveel meer geregeld, dan al was geregeld in de Wbp. Temeer opvallend dus dat de term Privacy by Design de laatste tijd overal wordt gebezigd in handreikingen waarmee organisaties zich kunnen voorbereiden op deze wettelijke verplichting die niet geheel nieuw is.

In dit afstudeerproject is onderzocht wat de actuele ontwikkelingen zijn op het gebied van Privacy by Design. In een tweetal case studies is onderzocht hoe informatie-intensieve organisaties in aanloop op de AVG omgaan met Privacy by Design en op welke wijze zij Privacy by Design implementeren.

2 Oorsprong van het concept Privacy by Design

Om dit onderzoek naar de actuele ontwikkelingen op het gebied van Privacy by Design beheersbaar te houden, is als uitgangspunt het oorspronkelijke concept van Privacy by Design genomen. Privacy by Design (PbD) is een concept dat Ann Cavoukian, een privacy functionaris uit Canada, in de jaren negentig ontwikkelde. PbD gaat ervan uit dat de bescherming van privacy nu en in de toekomst niet alleen gewaarborgd wordt door het naleven van wet- en regelgeving, maar dat de bescherming van privacy idealiter in de modus operandi van een organisatie besloten ligt.



Figuur 1. Privacy by Design – 7 foundational principles, https://bauhaus.nl/gdpr-privacy-by-design-in-praktijk/

De 7 fundamentele principes van PbD luiden, vertaald uit het Engels, als volgt:

1 *Proactief en niet reactief; Preventie, geen herstel*. De Privacy by Design aanpak wordt gekarakteriseerd door het nemen van proactieve in plaats van reactieve maatregelen.
2 *Privacy als Default (Privacy als Standaard)*. Er wordt van een individu geen actie verwacht om de eigen privacy te beschermen – deze bescherming is al in het systeem ingebouwd – standaard.
3 *Privacy is ingebed in het ontwerp*. Privacy by Design is ingebed in het ontwerp en de architectuur van IT-systemen en bedrijfsprocessen.
4 *Behoud van volledige functionaliteit; positieve som (win-win) in tegenstelling tot een nulsom*. Privacy by Design streeft naar een win-win situatie bij de ondersteuning van alle doelstellingen en belangen.
5 *End-to-end beveiliging – bescherming gedurende de hele levensduur*. Sterke beveiligingsmaatregelen zijn essentieel voor bescherming van privacy van begin tot eind.
6 *Zichtbaarheid en transparantie*. Privacy by Design wil alle betrokkenen ervan overtuigen dat, bij welke gebruikte werkwijze of toegepaste technologie dan ook, wordt gehandeld conform de gestelde beloften en afspraken.
7 Respect voor de privacy van de gebruiker - Stel de gebruiker centraal

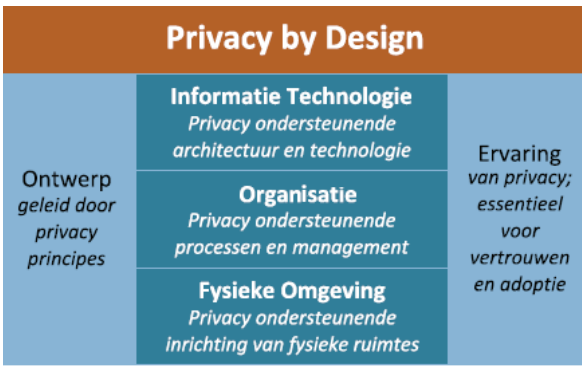
Ann Cavoukian heeft in 2012 een 'guide to implementing strong privacy practices' uitgebracht. Hieraan wordt verderop gerefereerd als 'best practices'.

3 Privacy by Design in Nederlandse richtlijnen en handreikingen

In het tijdbestek tussen het voorstel van de Europese Commissie voor een nieuwe wetgeving met betrekking tot persoonsbescherming tot heden verscheen in Nederland een aantal handreikingen van diverse organisaties waarin de term Privacy by Design invulling krijgt. Zij vormen een bruikbare bron voor verschillende organisaties in Nederland, die moeten voldoen aan de AVG.

TNO

In 2012 verscheen in Nederland van TNO een rapport 'Stimulerende en remmende factoren van Privacy by Design in Nederland' dat aansluit bij Ann Cavoukian's concept. TNO ziet PbD in tegenstelling tot de tot dan toe leidende Privacy Enhancing Technology (PET's) benadering, meer als een systemische benadering (van wieg tot wieg) waarbij ook niet-technische aspecten (procesmatige, organisatorische en ruimtelijke) nadrukkelijk worden betrokken bij de vormgeving van nieuwe diensten. Dit concept is opgebouwd uit bouwstenen zoals in Figuur 2 zijn weergegeven. In paragraaf 5.2 wordt verder ingegaan op PET's.



Figuur 2. Bouwstenen Privacy by Design uit 'Stimulerende en remmende factoren van Privacy by Design in Nederland'

Centrum voor Informatiebeveiliging en Privacybescherming
Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) is het expertisecentrum voor informatiebeveiliging en privacybescherming van, voor en door overheidsorganisaties. Het CIP heeft een aantal documenten uitgebracht in het kader van 'Grip op de Privacy' waaronder:

- Privacy Baseline - De AVG ontrafeld voor praktische toepassing in organisaties. Deze baseline bevat 13 criteria voor organisaties die persoonsgegevens verwerken.
- Handleiding Privacy by Design - Deze handleiding beschrijft hoe privacyaspecten direct meegenomen kunnen worden in de ontwerpfase van informatiesystemen en processen.
- Handleiding Borging van Privacy in organisaties en een Volwassenheidsmodel – Dit is een handleiding voor Privacy Governance.

KPMG - Ronald Koorn e.a.
In opdracht van het Ministerie van Binnenlandse Zaken schreven Ronald Koorn en andere KPMG collega's in 2004 Privacy Enhancing Technologies – witboek voor beslissers "om u te stimuleren PET toe te passen om persoonsgegevens veilig te verwerken". Ronald Koorn heeft tijdens de opleiding een college over privacy verzorgd.

Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens (AP), tot 1 januari 2016 bekend als College Bescherming Persoonsgegevens (CPB), houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. Een andere belangrijke taak van de AP is het adviseren over nieuwe regelgeving. De AP heeft de bevoegdheid om organisaties boetes op te leggen bij overtreding van de privacy wetgeving.
In de richtsnoeren beveiliging van persoonsgegevens uit 2013 spreekt het CBP van beveiliging die past binnen het breder verband van Privacy by Design, waarbij de bescherming van persoonsgegevens en de borging van de rechten van de betrokkenen vanaf het allereerste begin in de informatiesystemen wordt ingebouwd. Volgens het CBP zijn Privacy Enhancing Technologies bij dergelijke verwerkingen onmisbaar. Het CBP verwijst hierbij naar het witboek van Ronald Koorn e.a. In de publicaties op de website van de AP ter voorbereiding van de AVG, waaronder 'het AVG- 10 stappenplan', komen Privacy Enhancing Technologies nergens meer terug.

Privacy & Identity Lab - Jaap-Henk Hoepman
Jaap-Henk Hoepman is hoofddocent privacy enhancing technologies en identity management aan de Radboud Universiteit en stond in 2011 aan de wieg van het Privacy & Identity Lab. Sinds 2014 is hij de wetenschappelijk directeur. De afgelopen jaren verscheen van zijn hand een aantal artikelen over het toepassen van Privacy by Design bij het ontwikkelen van systemen.

NOREA
De beroepsorganisatie van IT-Auditors, NOREA, brengt in februari 2013 een informerende publicatie 'Het Europees privacyrecht in beweging' uit, in samenwerking met Duthler Associates en Kluwer. "Nieuw in de verordening zijn de Privacy by Design en Privacy by Default eisen" constateert NOREA. NOREA stelt dat "de vereisten van Privacy by Design en Privacy by Default nog niet uitgekristalliseerd zijn, maar dat op basis van het kader 'met inachtneming van de stand van de techniek en de uitvoeringskosten' datgene dat technisch afdwingbaar is, ook technisch geïmplementeerd dient te worden".
In september 2017 verscheen in 'De IT-Auditor' een nieuw Privacy Control Framework waarin de 31 meest genoemde, en waarschijnlijk wereldwijd meest toegepaste, privacy beheersmaatregelen in een volledig en samenhangend beeld zijn samengebracht. Als één van de privacy control domeinen wordt *Privacy Architectuur (Privacy-by-Design) genoemd.*

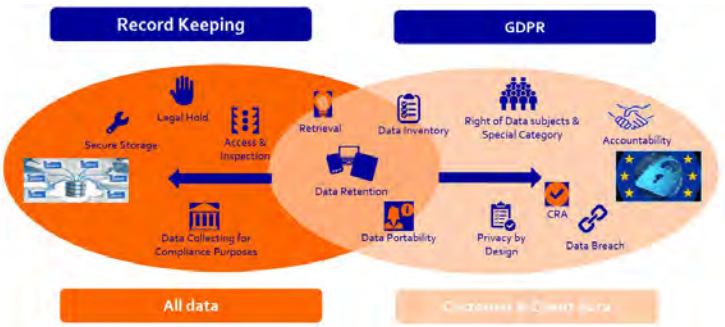
Verdonck, Klooster & Associates
Verdonck, Klooster & Associates (VKA) is een strategisch ICT-adviesbureau. In juni 2017 geeft VKA een boekje uit, 'Privacy by Design' genaamd. Dit boekje is geschreven door Frank van Vonderen en biedt een helpende hand aan organisaties die bezig zijn met PbD. Alhoewel Privacy by Design nog geen concreet toepasbaar concept is, is het wel concreet te maken, aldus VKA. In het boekje komen concrete herkenbare ervaringen bij klanten ten aanzien van PbD aan de orde.

4 Achtergrond van de case studies

De case studies zijn uitgevoerd bij de Rabobank en de Sociale Verzekeringsbank (SVB). Beide organisaties vervullen een maatschappelijke rol in het leveren van diensten. Of het nu gaat om het leveren van kredieten of het leveren van sociale voorzieningen, beide organisaties hebben te maken met een enorme hoeveelheid aan persoonlijke gegevens, die noodzakelijk zijn voor het uitvoeren van hun primaire taak.

In Nederland bedient de Rabobank ruim 6,7 miljoen Nederlandse particuliere en 800.000 zakelijke klanten met een compleet pakket aan financiële producten en diensten. Internationaal is de Rabobank vooral actief als financiële dienstverlener in de landbouw en voedingssector. Wereldwijd is Rabobank actief in veertig landen en bedient zij circa 10 miljoen klanten.

Ten tijde van dit onderzoek was een tweetal programma's actief bij de Rabobank met als doelstelling om compliancy voor GDPR te bewerkstelligen: de programma's GDPR en Record Keeping. De implementatie van de GDPR is onderverdeeld in werkpakketten, gebaseerd op de onderwerpen van de GDPR en het onderscheid tussen klant en medewerker. Privacy by Design is één van de werkpakketten binnen het programma GDPR, waarbij het er om gaat te implementeren dat elk nieuw systeem, product, contract en proces, dat gebruik maakt van persoonlijke data de bescherming van die data in overweging moet nemen. Privacy hoort ingebed te zijn in de opzet; adequate beveiliging moet geregeld zijn en de compliance moet gemonitord worden. Het programma Record Keeping is opgestart om een beleid te definiëren en te implementeren waarmee Rabobank voldoet aan de geldende wet- en regelgeving met als doel het bewaren, ophalen, veilig opslaan en vernietigen van records, het (tijdelijk) bevriezen van records vanuit juridisch oogpunt (Legal hold), het verzamelen van data voor compliance doelstellingen en toegang en inspectie van data door Toezichthouders. De twee programma's hebben voornamelijk een overlap voor wat betreft dataretentie zoals Figuur 3 aangeeft. De GDPR-wetgeving vereist het inrichten van bewaartermijnen en de naleving en het programma Record Keeping zorgt voor de implementatie hiervan.



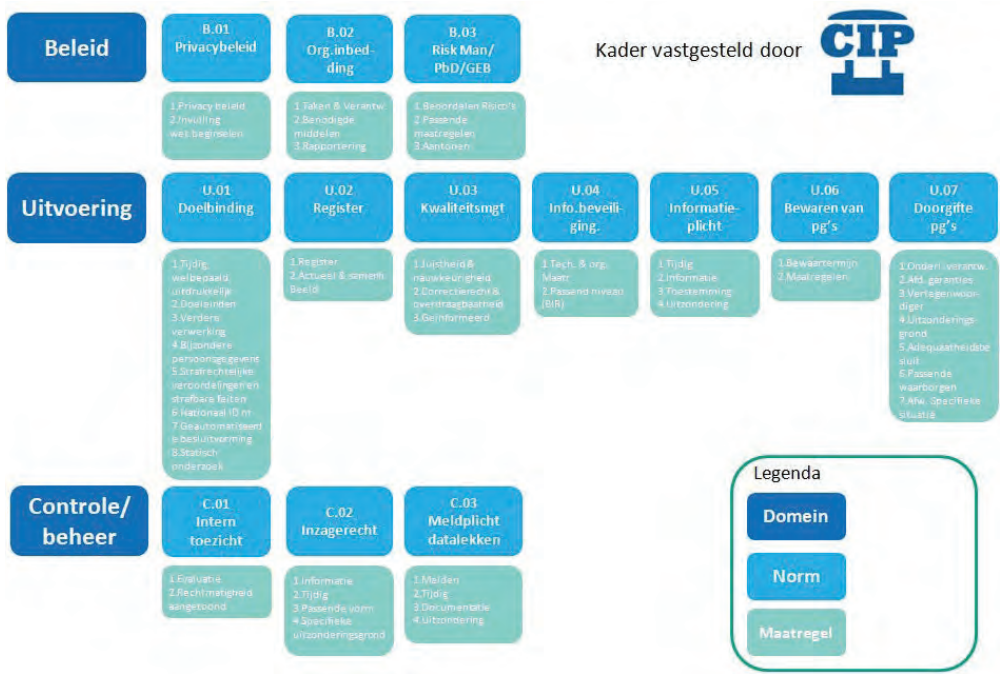
Figuur 3. Rabobank Programma's Record Keeping en GDPR met het werkpakket Privacy by Design

Eind 2017 heeft de SVB 3.422.100 AOW (Algemene Ouderdomswet) gerechtigden in de systemen waarvan 338.300 gerechtigden in het buitenland wonen, 1.908.383 huishoudens met 3.363.161 kinderen die kinderbijslag ontvangen, waarbij 39.956 kinderen in het buitenland wonen en 123.941 personen die een persoonsgebonden budget ontvangen

Het ministerie van SZW, de belangrijkste opdrachtgever van de SVB, heeft in juni 2017 per brief gevraagd om een uitvoeringstoets op de Algemene Verordening Gegevensbescherming uit te voeren, waarbij expliciet wordt aangegeven dat “voor de ontwikkeling van nieuwe gegevensverwerkende systemen het principe van **Privacy by Design** gevolgd dient te worden”.

In een uitvoeringstoets geeft de SVB een oordeel over de consequenties van wijzigende wet- en regelgeving voor de uitvoering en de consequenties voor de klant In de uitvoeringstoets geeft de SVB aan te kiezen voor de Privacy Baseline van het Centrum Informatiebeveiliging en Privacybescherming als leidraad voor de impactbepaling. De SVB spreekt de verwachting uit, dat per mei 2018 het principe van Privacy by Design is geborgd in de processen en dus zal worden meegenomen in alle nieuw te bouwen systemen vanaf mei 2018.

Voor het aansturen van het project ‘implementatie AVG’ is een externe projectmanager aangetrokken. Hij heeft het project opgesplitst in werkpakketten die in lijn liggen met de normen uit de handreiking van het CIP. In het project wordt veelvuldig gebruik gemaakt van een model van de werkpakketten dat is gebaseerd op de Privacy Baseline, zoals in Figuur 4 is afgebeeld.



Figuur 4. Model gebaseerd op de CIP Privacy Baseline

5 Uitwerking per Privacy by Design principe

Paragrafen 5.1 tot en met 5.7 zijn gestructureerd aan de hand van de 7 fundamentele principes van Privacy by Design die zijn weergegeven in hoofdstuk 2.

5.1 PbD principe 1: Proactive not Reactive; Preventive not Remedial

Om als bedrijf in staat te zijn om een proactief privacy programma uit te voeren, moeten bepaalde randvoorwaarden zijn ingevuld. In haar best practices noemt Ann Cavoukian allereerst de betrokkenheid van het hoger management. Betrokkenheid blijkt volgens haar niet alleen uit privacybeleid. Binnen een organisatie moet voldoende bewustwording worden gecreëerd in een cultuur van voortdurende verbetering. Er moet een systematische methode worden ontwikkeld voor het inschatten van risico's en het wegnemen van negatieve impact. Frank van Vonderen verwoordt dat als volgt: "Privacy by Design is veel meer een vaardigheid die door uw organisatie constant moet worden ingezet. […] Het is meer een roeping of way-of-life, zo je wilt".

De wetgeving rept in vele artikelen over "passende organisatorische" maatregelen, om de rechten en vrijheden van de betrokkene te beschermen, om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de verordening wordt uitgevoerd, om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn, etc. Die maatregelen moeten volgens de wet worden geëvalueerd en indien nodig geactualiseerd.

TNO, de Autoriteit Persoonsgegevens en het CIP noemen alle drie bewustwording als belangrijk aspect van privacybescherming. In de interpretaties van de nieuwe AVG wetgeving heeft de AP op haar website de 10 belangrijkste stappen op een rijtje gezet ter voorbereiding op de komst van de AVG. Als stap 1 formuleert de AP: bewustwording. De AP waarschuwt in stap 1 ook voor mogelijke sancties als men zich niet aan de nieuwe privacywetgeving houdt.
Het CIP ziet het privacybeschermingsprogramma als veranderprogramma. De veranderstrategie zou zich moeten richten op het betrekken van de staande organisatie bij het formuleren van ambities, korte en lange termijn doelen, en een geleidelijke en "haalbare" groei. De aard van het onderwerp 'privacy' rechtvaardigt een dergelijk "menselijke maat aanpak" boven het eenzijdig van bovenaf vaststellen van termijndoelen in een resultaat gerelateerd afrekenmodel.

Case study

Binnen de SVB is het project AVG gestart met het inventariseren van alle binnen de SVB aanwezige beleidsstukken die bij de overgang van de Wbp naar de AVG aangepast moeten worden. En ook binnen de Rabobank luidt het eerste leidende principe van het werkpakket PbD in het programma GDPR: "Privacy by Design applies from the initiation of the design and not afterwards. Starting with Privacy at Design is already starting with policy making". In beide organisaties worden vele beleidsstukken aangepast.

In de 'Global Standard on Privacy by Design' van de Rabobank is opgenomen, dat er verwacht wordt dat alle Rabobankmedewerkers op alle niveaus van de Rabobank Groep de meest ondersteunende rol zullen moeten aannemen om effectief en efficiënt 'Privacy by Design' principes te integreren bij de Rabobank. Daarnaast wordt er verwacht dat elke Rabobankmedewerker in de dagelijkse activiteiten en scope van verantwoordelijkheden een proactieve en preventieve houding aanneemt met betrekking tot data privacy. Binnen de SVB zijn zowel in de functiebeschrijving van de Functionaris Gegevensbescherming als van de privacycoördinator taken opgenomen met betrekking tot het creëren van awareness. Een opvallende taak van de privacycoördinator is "het creëren van een sfeer waarin privacy leuk is en kansen creëert".

Privacybescherming als een 'way-of-life' zou in grote mate helpen bij de groei in PbD-volwassenheid. Zowel binnen de Rabobank als binnen de SVB wordt privacybescherming langzamerhand ingebed in de dagelijkse activiteiten. Het thema privacy zal een terugkerend item moeten worden op de agenda van het hogere management, om groei naar volwassenheid in Privacy by Design te blijven bewerkstelligen.

5.2 PbD principe 2: Privacy as the default setting

Artikel 25 van de AVG wetgeving gaat in op gegevensbescherming door ontwerp en door **standaardinstellingen**.

Er lijken twee zienswijzen te bestaan op Privacy by Default:

1. Privacy by Default gaat over het gebruikmaken van configuratie-instellingen in een systeem, app, website of een dienst en deze zo privacy-vriendelijk mogelijk instellen.

Een legendarisch voorbeeld waarbij dit niet het geval was, haalt Van Vonderen aan in zijn boekje Privacy by Design namelijk het beruchte Project-X-feest in Haren, waarbij een meisje door een foutje met privacy-opties op Facebook een openbare uitnodiging plaatste voor haar sweet sixteen party, waarna deze uitnodiging viraal ging. Duizenden jongeren verschenen daadwerkelijk. Was de standaardinstelling niet 'openbaar' geweest, dan had het in Haren wellicht niet zo gemakkelijk uit de hand gelopen.

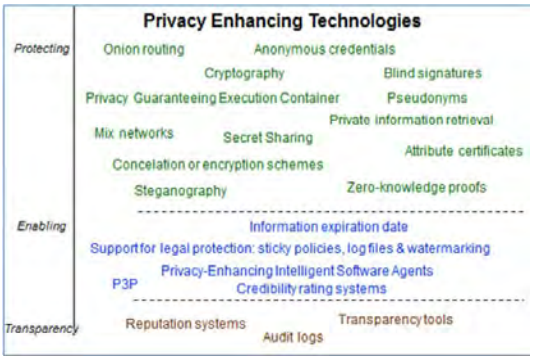
2. Privacy by Default gaat over het voldoen aan de verwachting van de klant die ervan uit mag gaan dat zijn privacy in IT-systemen en handelingspraktijken standaard afdoende is beschermd.

Ann Cavoukian zegt hierover in haar best practices: "We want to encourage thinking beyond the default settings associated with preferences that users can manually control, and to consider the overall system defaults".

Als men denkt aan "overall system defaults", dan gaat het ook om het integreren van technische maatregelen in het IT-systeem die de privacy kunnen bevorderen. Met Privacy Patterns en Privacy Enhancing Technologies kan hieraan een goede invulling worden gegeven.

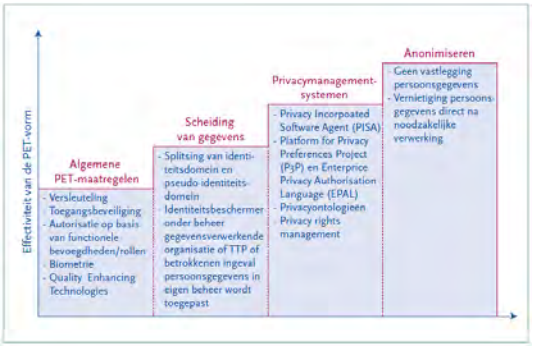
Privacy Patterns en Privacy Enhancing Technologies (PET's)
Het concept Design Patterns komt van origine uit het programmeren met object georiënteerde software. Design patterns hebben als eigenschap dat ze hergebruikt kunnen worden en een gestandaardiseerde manier van vastlegging hebben. Daarmee hebben systeemontwikkelaars de mogelijkheid om herhaaldelijk optredende problemen van dezelfde soort tijdens de systeemontwikkeling op te lossen. In de context van privacy noemt men design patterns, privacy patterns. Op de website privacypatterns.org zijn vele voorbeelden van privacy patterns te vinden, zoals het standaard softwareontwerp "Use of dummies" om activiteiten van een gebruiker te verbergen door het toevoegen van nepacties, die niet van echt te onderscheiden zijn.

Daar waar patterns veelal betrekking hebben op software- en systeemontwikkeling en gebruikt kunnen worden tijdens het programmeren van verschillende aspecten van Privacy by Design, zijn PET's meer technische functionaliteiten die min of meer off-shelf toegepast kunnen worden. TNO deelt PET's in op basis van een drietal functionele aspecten namelijk: Privacy Protecting, Enabling en Transparency tools (zie Figuur 5).



Figuur 5. Overzicht van technische tools en maatregelen om privacy te beschermen uit 'Stimulerende en remmende factoren van Privacy by Design in Nederland'

Koorn e.a. onderscheiden in het witboek vier hoofdvormen van PET's om deze daarna te vergelijken op basis van effectiviteit. De effectiviteit van deze hoofdvormen van PET's, wordt door de auteurs weergegeven in een zogenaamde PET-trap (Zie Figuur 6).



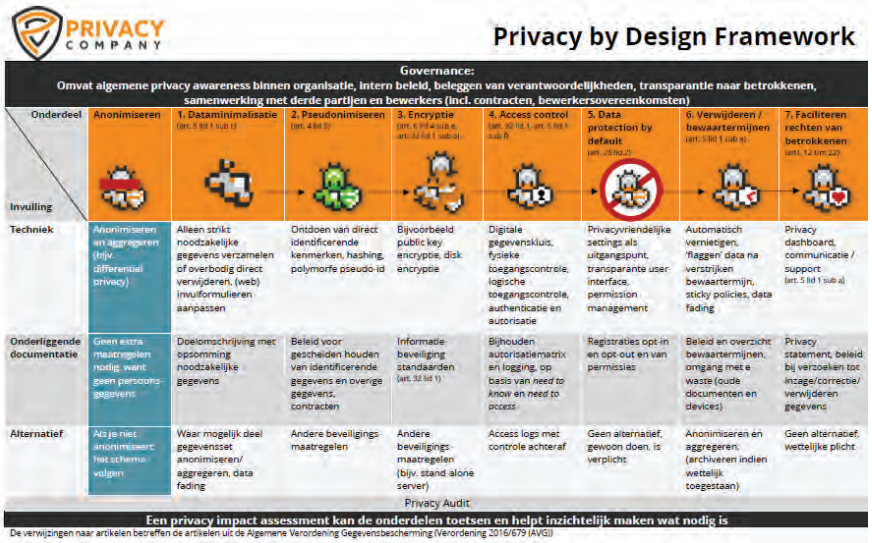
Figuur 6. PET-trap: de effectiviteit van PET-vormen uit 'Privacy Enhancing Technologies - Witboek voor beslissers'

Case study

Bij de Rabobank is "Privacy as the default setting" in het beleid opgenomen in de Global Standard on Privacy by Design. Hierbij gaat het over het voldoen aan de verwachting van de klant, die ervan uit mag gaan dat zijn privacy in IT-systemen en handelingspraktijken standaard afdoende is beschermd. Dit is gelijk aan de zienswijze van Ann Cavoukian. Het programma GDPR heeft in het werkpakket PbD als één van de 7 leidende principes: "Privacy criteria apply by default. In addition, the rule is 'comply or explain'". Concrete invulling door (technische) maatregelen beperkt zich tot de deliverable 'Anonimisering en Pseudonimisering'. Het GDPR-programma heeft reeds een Global Standard ontwikkeld voor anonimiseren en pseudonimiseren. In deze standard wordt aangegeven hoe de Rabobank hiermee moet omgaan en welke procedures ervoor gevolgd moeten worden. Daarnaast wordt er aandacht besteed aan een technische tool ten behoeve van datamasking, die door de organisatie gebruikt kan worden.

De SVB beschouwt Privacy by Design met name als iets dat in ICT-systemen ingebouwd wordt. Deze invulling sluit ook aan bij het tweede principe van Ann Cavoukian: privacybescherming is al in het systeem ingebouwd - standaard. Het AVG project heeft de uitgangspunten voor 'Privacy by Design & Privacy by Default'

geformuleerd en gebruik gemaakt van het Privacy by Design Framework van de Privacy Company. De Privacy Company heeft het principe van Privacy by Design in dit Framework samengevat in een eenvoudig te volgen stappenplan, dat in volgorde van aangegeven stappen doorlopen moet worden, en waarbij ook alternatieven worden geboden, zie Figuur 7.



Figuur 7. PbD Framework https://www.privacycompany.eu/files/Privacy%20by%20Design%20Framework.pdf

Het project AVG heeft aansluiting gezocht tussen de onderdelen van het PbD framework en de reeds binnen de SVB aanwezige beleidsuitgangspunten en kaders. Op die manier is een analyse gemaakt van gaps om deze vervolgens te adresseren. Een concrete invulling betreft een apart project dat zich bezighoudt met de datamasking van de gegevens op de testomgevingen. Hiervoor wordt gebruik gemaakt van een tool.

Zowel bij de Rabobank als de SVB is er met name sprake van een 'opzet' van IT Privacy by Design maatregelen. Beide organisaties werken concreet aan anonimisering en pseudonimisering met behulp van datamasking tooling, een voorbeeld van Privacy Enhancing Technology.

5.3 PbD principe 3: Privacy embedded into Design

Privacy Impact Assessment

Het derde Privacy by Design principe van Ann Cavoukian luidt dat 'privacy is ingebed in het ontwerp en de architectuur van IT-systemen en bedrijfsprocessen'. Principe 3 is verdeeld in de onderwerpen PIA (ook genoemd: Privacy Risk Assessment, Gegevensbeschermingseffectbeoordeling (GEB), Dataprotection Impact Assessment) en architectuur. Ann Cavoukian introduceert een Privacy Risk Assessment als onderdeel van de ontwerpfase van elk nieuw initiatief. De IT-architectuur geeft vervolgens richting aan de te nemen maatregelen binnen het IT-landschap. Het resultaat hiervan is dat privacy een integraal onderdeel is van de geleverde functionaliteit.

Artikel 35 van de AVG introduceert in dit kader de 'Gegevensbeschermingseffectbeoordeling', beschrijft wat deze inhoudt en wanneer deze verplicht is. De GEB wordt omschreven als een "beoordeling […] van

het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens“. Het gaat dus om een voorafgaande analyse van de gevolgen voor privacy van een verwerking van persoonsgegevens.

Het CIP geeft in haar ‘Handleiding Privacy by Design’ aan dat bij het verwerken van persoonsgegevens een GEB verplicht is, maar ook bij verdere verwerking van die gegevens. Om de verschillende situaties te onderscheiden en daarbij een pragmatische oplossing te bieden voor het wel of niet uitvoeren of uitbreiden van een GEB, maakt het CIP onderscheid in de aard van de verwerking (incidenteel of structureel) en of deze verwerking (wel of niet) conform of verenigbaar is met het oorspronkelijke doel.

Het PIA-toetsmodel van de Rijksdienst stamt uit september 2013 en is recentelijk in september 2017 vernieuwd. Het nieuwe Model Gegevensbeschermingseffectbeoordeling Rijksdienst bestaat uit 3 onderdelen. Het eerste deel ‘Proceskader’ geeft een algemene inleiding op het instrument PIA en beschrijft het proces van het uitvoeren van een PIA. Het tweede deel ‘Model’ bevat het daadwerkelijke model om een PIA uit te voeren. In het derde deel ‘Toelichting’ wordt er toelichting gegeven op het model. Het toetsmodel hanteert een open vraag methodologie waarbij veelal om de beoordeling, motivatie en beschrijving wordt gevraagd. Een voorbeeld hiervan is: Rechten van de betrokkenen - Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen.

NOREA heeft een handreiking PIA (versie 1.2 - november 2015) uitgebracht, die organisaties kunnen gebruiken bij het uitvoeren van een Privacy Impact Assessment. NOREA heeft de te beantwoorden vragen gerelateerd aan privacy principes zoals: Limitering van het verzamelen van gegevens, Gegevenskwaliteit en Doelbinding en hanteert een gesloten vraag methodiek waarop Ja of Nee geantwoord kan worden. Een voorbeeld is: “Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?”.

De AP verwijst nog naar het oude PIA-toetsmodel van de Rijksdienst. Daarnaast is een verwijzing naar de ‘Guidelines on Data Protection Impact Assessment’ (door Article 29 Data Protection Working Party) pas in oktober 2017 toegevoegd aan de website van de AP, nadat deze was uitgekomen.

Case study

Bij de Rabobank wordt in het GDPR-programma in het werkpakket PbD veel aandacht besteed aan deliverables voor het uitvoeren van risicoanalyses. Dit behelst onder andere het beschikbaar maken van GDPR-compliant PIA’s. Een voorbeeld is een GDPR-compliant Product & Services PIA waarbij er een privacycheck plaatsvindt op nieuwe producten en diensten van de Rabobank en een PIA proces voor contracten met leveranciers. Daarnaast zijn er deliverables opgenomen om PIA’s centraal te loggen, KPI’s te definiëren en PDCA-cycli voor assessments in te regelen.

De SVB ziet de PIA als een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen om vervolgens maatregelen te kunnen nemen om de risico’s te verkleinen. Op deze manier kan de SVB voldoen aan de documentatieplicht en de verantwoordingsplicht.
Binnen de SVB is een PIA-proces gedefinieerd, waarin is opgenomen dat in een zo vroeg mogelijk stadium, namelijk in de ontwerpfase van de gegevensverwerking, moet worden gestart.
De SVB heeft voor de Privacy Impact Assessment een Template PIA SVB gedefinieerd. Dit template is gebaseerd op het Model Gegevensbeschermingseffectbeoordeling van de Rijksoverheid. De Functionaris Gegevensbescherming van de SVB geeft aan dat zij de uitvoering van PIA’s ziet als een belangrijk instrument om toezicht te houden. Men is nu vooral nog zoekende hoe de toezichtfunctie in te vullen met geschikte toezichtsinstrumenten.

Zowel de Rabobank als de SVB voeren al jarenlang Privacy Impact Assessments uit, onder andere bij nieuwe projecten. De processen hieromtrent worden, vooruitlopend op de AVG, aangepast om te voldoen aan de nieuwe wetgeving.

Architectuur
Onder Privacy Impact Assessment is uiteengezet op welke wijze een assessment van de privacyrisico's in een vroeg stadium de privacy impact op onder meer het IT-landschap en de te nemen maatregelen, duidelijk maakt. De IT-architectuur geeft vervolgens richting aan de te nemen maatregelen binnen het IT-landschap.

In de nieuwe wetgeving komt de term architectuur niet voor.

Wel zijn in de 'Privacy Design Strategies' uit 2012 van Hoepman uitgangspunten vanuit de wetgeving te herkennen zoals Doelbinding (purpose limitation), Minimale gegevensverwerking (data minimisation), Juistheid van gegevens, Rechten van de betrokkene, Voldoende Bescherming en Verantwoordingsplicht (Zie Tabel 1).

	Purpose limitation	Data minimisation	Data quality	Transparency	Data subject rights	The right to be forgotten	Adequate protection	Data portability	Data breach notification	(Provable) Compliance
MINIMISE	o	+								
HIDE		+					o			
SEPARATE	o						o			
AGGREGATE	o	+								
INFORM				+	+				+	
CONTROL			o		+			+		
ENFORCE	+		+			+	+			o
DEMONSTRATE										+

Legend: +: covers principle to a large extent. o: covers principle to some extent.

Tabel 1. Mapping of strategies onto legal principles uit 'Privacy Design Strategies (extended abstract)' in IFIP TC11 29th Int. Conf. on Information Security (IFIP SEC 2014), June 2014

In zijn artikel 'Privacy Design Strategies' geeft Hoepman aan dat richtinggevende kaders nodig zijn om Privacy by Design vanaf de start van het ontwikkelproces mee te kunnen nemen. Deze helpen de IT-architect om invulling te geven aan Privacy by Design in de fasen van conceptontwikkeling en analyse. Hoepman definieert 8 privacy design strategieën:

Minimise strategy
Dit is de meest basale strategie waarbij de hoeveelheid persoonlijke informatie die verwerkt wordt, zo beperkt mogelijk is. Door geen of alleen het hoogstnoodzakelijke aan persoonlijke informatie te verzamelen

Hide strategy
Bij de Hide strategie gaat het om het uit het zicht houden van persoonlijke informatie die wordt verwerkt.

Separate strategie
De Separate strategie schrijft voor dat het verwerken van persoonlijke informatie waar mogelijk zal geschieden op gedistribueerde wijze. Door het scheiden van de opslag of de verwerking van meerdere bronnen van persoonlijke gegevens die bij één persoon horen, kan er geen compleet profiel van de persoon gecreëerd worden.

Aggregate strategy
Persoonlijke informatie wordt verwerkt op het hoogste niveau van aggregatie en met het minst mogelijke, nog steeds bruikbare, detail.

Inform strategy
Personen moeten voldoende vooraf geïnformeerd zijn als hun persoonlijke informatie wordt verwerkt.

Control strategy
De Control strategie geeft aan dat personen de regie moeten kunnen hebben over de verwerking van hun persoonlijke gegevens.

Enforce strategy
Deze strategie zorgt ervoor dat een systeem, zowel tijdens ontwikkeling als in productie, conform gegevensbeschermingswetgeving functioneert.

Demonstrate strategy
De laatste strategie vereist dat een verwerkingsverantwoordelijke in staat is om aan te tonen dat het privacybeleid en de wettelijke vereisten worden nageleefd.

In het artikel 'A critical Analysis of Privacy Design Strategies' uit 2016 van Colesky, Hoepman en Hillen wordt naast privacy design strategie, het begrip 'tactics' geïntroduceerd. Deze tactics vormen een abstractie laag tussen een privacy design strategie en patterns en geven invulling aan de strategie.

MINIMISE	HIDE	SEPARATE	ABSTRACT
EXCLUDE SELECT STRIP DESTROY	RESTRICT MIX OBFUSCATE DISSOCIATE	DISTRIBUTE ISOLATE	SUMMARIZE GROUP
INFORM	**CONTROL**	**ENFORCE**	**DEMONSTRATE**
SUPPLY NOTIFY EXPLAIN	CONSENT CHOOSE UPDATE RETRACT	CREATE MAINTAIN UPHOLD	AUDIT LOG REPORT

Tabel 2. Strategies by Tactics uit 'A Critical Analysis of Privacy Design Strategies'.

Twee voorbeelden zijn de tactic Exclude die invulling geeft aan de Minimise Strategy en die inhoudt dat geheel of gedeeltelijk wordt afgezien van het verwerken van de persoonlijke gegevens van een persoon en de tactic Dissociate die invulling geeft aan de Hide Strategy en waarbij de correlatie tussen verschillende onderdelen van persoonlijke gegevens wordt verwijderd.

Met betrekking tot een concrete invulling van privacybescherming, bijvoorbeeld het niet onnodig tonen van vertrouwelijke gegevens aan verwerkers, binnen een architectuur verwijst het CIP naar een meerlagen architectuur, namelijk:

1 *Procesbesturingslaag*: een beschrijving van een geordende reeks van processtappen die in z'n geheel bij één verantwoordelijke of organisatorische eenheid belegd kan worden om een specifieke bijdrage te leveren bij de verwerking van persoonsgegevens.

2 *Verwerkingslaag*: in de verwerkingslaag is de functionaliteit van de applicatie ondergebracht. De functionaliteit bestaat bijvoorbeeld uit verwerkingslogica met daarin de business logica.
3 *Gegevenslaag*: in een gegevenslaag zijn die gegevens ondergebracht die worden bewerkt in de verwerkingslaag.

Een meerlagen technische architectuur ondersteunt het implementeren van de juiste granulariteit, waarmee toegang 'op maat' bereikt kan worden.

Het CIP adviseert om per gegevensverwerkingsdoel maximaal één voorziening/applicatie te gebruiken. Ook is het belangrijk om bij het ontwerp van systemen de complexiteit van gegevensverwerkingen beperkt te houden, door het aantal terugkoppelingen (lussen) dat zich in de procesflow van de gegevensverwerking bevindt, te beperken. Persoonsgegevens worden zoveel mogelijk geautomatiseerd verwerkt volgens formeel bepaalde logica zoals business rules in een Business Rule Managementsysteem (BRM) en door de toewijzing van gegevens waarbij handmatige acties nodig zijn, te regelen via een Workflow Management Systeem (WMS).

Case Study

In 2014 is de architectuurafdeling binnen Rabobank betrokken geweest bij Privacy by Design. Men realiseerde zich toen dat het starten met PbD vanaf architectuur te laat was. Over PbD moet nagedacht worden bij de business, dit is de reden waarom er in 2014 is besloten om een PbD policy te ontwikkelen, waarmee de business rekening kon houden. Het resultaat is de Global Standard on Privacy by Design waarin is opgenomen dat privacy al begint bij het toepassen van Privacy by Design principes in de business case.

De architecten binnen SVB zijn niet actief betrokken bij het project dat de AVG implementeert. De verwachting van de architecten is dat op termijn Privacy by Design zal worden uitgekristalliseerd in regelgeving en zal worden gestandaardiseerd. De markt zal hierop inspelen door het ontwikkelen van tooling die toepassingen van Privacy by Design zal ondersteunen. Tegen die tijd zullen, op aangeven van de business en in overleg met de Functionaris Gegevensbescherming, bindende architectuurkaders ontstaan.

5.4 PbD principe 4: Full functionality, Positive Sum (win-win), not Zero Sum

In de speltheorie zijn positive-sum, win-win en zero-sum termen die refereren aan de opbrengsten of verliezen van één speler ten opzichte van de opbrengsten of verliezen van de andere speler(s). Binnen principe 4 is privacybescherming de ene 'speler' en andere functionaliteiten zoals beveiliging of performance zijn de andere 'speler'. Een win-win situatie is een bijzonder positive-sum uitkomst waarbij het totaal aan verbeteringen groter dan 0 is, en waarbij zowel de privacybescherming als de overige functionaliteit is verbeterd. Volgens Ann Cavoukian is het met samenwerken en innovatieve oplossingen mogelijk om zowel verbetering op het gebied van privacybescherming als verbetering op het gebied van alle andere gewenste functionaliteiten te bereiken.

De wetgeving zegt in preambule (4) over belangenafweging het volgende: "De verwerking van persoonsgegevens moet ten dienste van de mens staan. Het recht op bescherming van persoonsgegevens heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen".

In een kritisch artikel 'How is Positive-sum Privacy Feasible?' [Bier, C. e.a. 2012] omschrijven de auteurs de 7 principes van Ann Cavoukian als 'nogal abstract van aard en moeilijk in de praktijk toe te passen'. Met name het vierde PbD principe is volgens de auteurs 'twijfelachtig', zowel in theoretisch als in praktisch opzicht.

Wanneer men start vanuit de theoretische situatie van volledige privacy en geen functionaliteit, zo betogen de auteurs, dan betekent het toevoegen van functionaliteit waarbij persoonsgegevens nodig zijn noodzakelijkerwijs dat de privacybescherming afneemt. Het bepalen, bovendien, of er sprake is van een zero-sum, positive-sum dan wel win-win situatie vereist het meten van de mate van privacy en de mate van de andere functionaliteiten, het prioriteren ervan en het aanbrengen van een weging. Voor deze zaken is vooralsnog geen eenduidige methode gevonden.

Case Study

De Chief Privacy Officer van de Rabobank geeft aan dat dit principe niet letterlijk is overgenomen in de leidende PbD principes voor de Rabobank, omdat er geen goede vertaling voor gevonden kon worden. In een ronde tafel met Privacy Officers waarvan hij deel uitmaakt, kwam dit onderwerp aan de orde. Er kon geen goede invulling aan dit principe worden gegeven. Tijdens de discussie kwam ook naar voren dat het kwantificeren bij het bepalen van de Positive-Sum, not Zero-Sum lastig lijkt, omdat je onder andere aan het begin van een implementatie zit.

Binnen de SVB is het principe Positive-Sum geen specifiek aandachtspunt van het AVG project. Binnen de SVB spelen echter, net als binnen de Rabobank, wel degelijk meerdere bedrijfsbelangen die met het oog op privacy van klanten mogelijk op gespannen voet met elkaar staan. Eén van de leden van de RvB van de SVB verwoordt het in een artikel op www.socialevraagstukken.nl als volgt: “Bij de SVB willen we er niet alleen zijn om uitkeringen te verzorgen, maar ook om armoede te voorkomen en bestaanszekerheid te creëren. Dat is immers de bedoeling van de wetten die wij uitvoeren. […] Helaas lijkt hier bijvoorbeeld de privacywetgeving in de weg te staan en daarover zijn we in gesprek met de Autoriteit Persoonsgegevens”. Binnen de SVB werkt een multidisciplinair team sinds vorig jaar met data analytics. Het team heeft gewerkt aan een Schuldensignaleringsmodel waarmee met een hoge betrouwbaarheid kan worden voorspeld bij wie zich problematische schulden (zullen gaan) voordoen, zodat ingegrepen kan worden. Dit model wordt momenteel vanwege de privacywetgeving niet in de praktijk ingezet.

Naast deze geluiden over de belemmeringen van de privacywetgeving bij bijvoorbeeld het voorkomen van armoede, klinken er binnen de SVB ook meer voorzichtige geluiden. Deze propageren het betrachten van uiterste zorgvuldigheid bij het gebruik van persoonsgegevens. In dit verband wordt vaak ‘data ethics’ genoemd. Data ethics is een nieuwe vorm van ethiek die zich bezig houdt met de morele problemen gerelateerd aan o.a. het genereren, opslaan, delen etc. van gegevens en algoritmes, zoals machine learning en robotics met als doel om moreel goede oplossingen te formuleren en te ondersteunen.

5.5 PbD principe 5: End-to-end Security – Full Lifecycle Protection

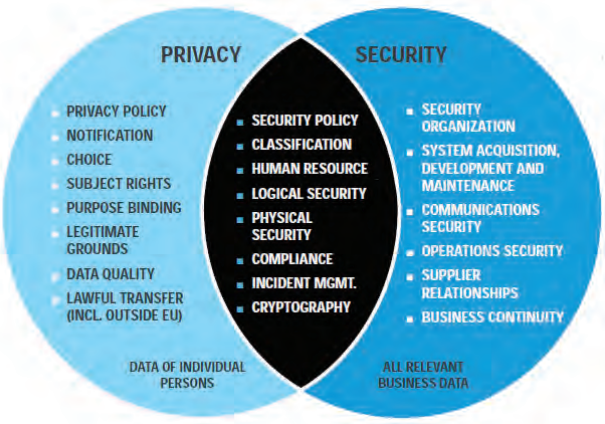
Nadat persoonsgegevens zijn verzameld, zo minimaal mogelijk en altijd met een wettelijke grondslag en duidelijke doelbinding, moeten deze persoonsgegevens tijdens de gehele levenscyclus worden beschermd. Dit is beschreven in het 5e PbD principe van Ann Cavoukian. Zij legt in het kader van end-to-end security de nadruk op encryptie en op de tijdige en veilige verwijdering van persoonsgegevens.

Artikel 32 van de AVG gaat over de beveiliging van de verwerking. De verwerkingsverantwoordelijke dient passende technische en organisatorische maatregelen te treffen om een, op het risico afgestemd, beveiligingsniveau te waarborgen. Concreet worden ‘pseudonimisering en versleuteling’ van persoonsgegevens genoemd. Daarnaast gaat Artikel 5 over het bewaren van persoonsgegevens en behandelt Artikel 17 het recht op gegevenswissing.

Met betrekking tot encryptie en de veilige verwijdering van vertrouwelijke gegevens, zoals persoonsgegevens, bijvoorbeeld van verwijderbare media, gaat het hier om duidelijke security maatregelen. Deze maatregelen komen ook ruimschoots aan bod in standaarden voor informatiebeveiliging als ISO 27001 en 27002 en de daarvan afgeleide Baseline Informatiebeveiliging Rijksdienst (BIR) die binnen de overheid gehanteerd wordt. Opvallend is dat in deze standaarden nauwelijks aandacht wordt besteed aan de beveiliging van specifiek persoonsgegevens.

Het CIP erkent dat informatiebeveiliging als doelstelling heeft om de beschikbaarheid, integriteit en de vertrouwelijkheid van de (verwerking) van gegevens, en daarmee persoonsgegevens, te waarborgen. Maar dit betekent volgens het CIP niet dat informatiebeveiliging per definitie ook de maatregelen neemt die gericht zijn op privacybescherming en daarbij op het waarborgen van de belangen van de betrokkene. Het CIP stelt dat beveiliging van persoonsgegevens om passende maatregelen vraagt. Deze maatregelen moeten zijn gedefinieerd op basis van een risicoanalyse waarin rekening wordt gehouden met verwerkingsrisico's zoals in artikel 32 van de AVG is verwoord.

Het verschil en de overlap tussen privacy en security worden duidelijk in het onderstaand model (Figuur 8).



Figuur 8. Privacy vs Security uit collegesheets 'Introduction to privacy & privacy auditing' door R. Koorn, september 2016

Dit model wil bijdragen aan het ontkrachten van het idee dat privacybescherming hetzelfde zou zijn als informatiebeveiliging. Privacybescherming vereist dus ook maatregelen die buiten de scope van security vallen.

Het CIP concretiseert voor de beveiliging van persoonsgegevens enkele maatregelen die, gezien de huidige stand van zaken (anno 2016), als passend moeten worden beschouwd, waaronder:

1 Authenticatie op een vertrouwde locatie vindt minimaal op basis van een kenniskenmerk plaats, dit is vaak een wachtwoord;
2 Er is een logging van het raadplegen van persoonsgegevens door beheerders (tijdstip en raadpleger);
3 Bijzondere persoonsgegevens worden versleuteld verstuurd, ook over een beveiligd netwerk binnen een organisatie.

Volgens TNO voegt de lifecycle bescherming het element van de verwijdering/vernietiging van gegevens toe. Hierdoor kan een spanning ontstaan tussen de levenscyclus van de aangeboden dienst en de gegevens die voor de dienst noodzakelijk zijn. Uitbreiding van een dienst met extra functionaliteiten (bijvoorbeeld op basis van nieuwe technologische mogelijkheden) kan tot een conflict leiden met het beleid rond gegevensverzameling en -gebruik.

VKA noemt in het boekje Privacy by Design: gooi weg wat je niet langer nodig hebt, waarbij ook wordt genoemd dat de database idealiter zo ontworpen wordt dat attributen onafhankelijk van elkaar kunnen worden verwerkt, gewijzigd en verwijderd.

Veel van de bestudeerde bronnen verwijzen met betrekking tot beveiliging van persoonsgegevens naar ISO 27001 en 27002. Men adviseert een risico gebaseerde aanpak die onderdeel uitmaakt van de dagelijkse gang van zaken middels een plan-do-check-act-cyclus.

Case study

De Rabobank gebruikt de internationale ISO/IEC 27001/27002 standaarden als bron voor het bepalen van de relevante security maatregelen. Daarnaast wordt bij de Rabobank een Security Risk Management Process (SRMP) gehanteerd om assets (systemen, infra diensten, leveranciers etc) voldoende te beveiligen tijdens de gehele levenscyclus. Dit proces wordt gebruikt om het risicoprofiel te bepalen en de mate van compliance met de Rabobank security baselines. Het SRMP kent de volgende fasen: Classificatie, Baseline compliance, Risk analysis en Risk Treatment (zie Figuur 9).

Figuur 9. Rabobank Security Risk Management Process

In het classificatie schema is privacy een onderdeel van vertrouwelijkheid in de BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid).

De Global Standard on Privacy by Design gaat in op: End-to-end security – Lifecycle Protection.
De Standard (gericht op gegevens) en het SRMP proces (gericht op informatiebeveiliging) geven op het gebied van het beleid handvatten ten aanzien van informatiebeveiliging en de bescherming van gegevens.

In het kader van de bescherming van persoonlijke gegevens worden in het programma GDPR en Record Keeping additionele specifieke maatregelen ontwikkeld zoals 'Rights of data subjects', 'anonimiseren en pseudonimiseren' en maatregelen zoals bewaren, ophalen, veilig opslaan en vernietigen van records.

De SVB past voor een afdoende beveiliging van (persoons)gegevens de Baseline Informatiebeveiliging Rijk (BIR) toe. De Chief Information Security Officer (CISO) is aangesteld en gemandateerd om informatiebeveiligingsmanagement binnen de SVB te definiëren, borgen en bewaken. Het CISO-team heeft de tactische normen uit de BIR geïntegreerd in de Security Policy SVB (SPS). Inmiddels is besloten om ook de beleidsnormen met betrekking tot privacybescherming onder de paraplu van de SPS te brengen, zodat het beleid voor alle medewerkers op één plek toegankelijk is. Er is inmiddels al een aantal specifieke zaken met betrekking tot privacybescherming toegevoegd, zoals de verplichting om een PIA uit te voeren bij verwerking van persoonsgegevens en de verplichting tot het afsluiten van verwerkersovereenkomsten. Het streven is om zo veel mogelijk invulling aan de privacyvereisten te geven vanuit bestaande bedrijfsprocessen zoals project- en changemanagement en leveranciersmanagement.

SVB valt onder de archiefwet. Volgens de archiefwet is de Raad van Bestuur van de SVB zorgdrager voor de archiefbescheiden van de SVB. De zogenoemde 'selectielijst' is de weergave van de bewaar- en vernietigingstermijnen die gelden voor de SVB. Vernietiging van digitale gegevens en documenten vindt binnen de SVB vooralsnog met name handmatig plaats. Als uitgangspunt voor de bouw van nieuwe ICT-systemen geldt vanaf 25 mei 2018 'Archiving by Design', dat wil zeggen dat al bij het ontwerp van nieuwe systemen wordt nagedacht over latere vernietiging van gegevens.

Beide organisaties maken voor de bescherming van persoonsgegevens gebruik van de bestaande informatiebeveiligingsorganisatie. Privacy-aspecten maken daarvan deel uit of worden daaraan toegevoegd.

5.6 PbD principe 6: Visibility and Transparency – Keep it open

Volgens Ann Cavoukian gaat het bij principe 6 om het overtuigen van betrokkenen dat er wordt gehandeld conform gestelde beloften en afspraken. Met betrekking tot de verwerking van hun persoonsgegevens hebben betrokkenen bepaalde rechten. Een bedrijf moet aan de betrokkenen transparantie kunnen bieden over de verwerking, zodat betrokkenen deze rechten kunnen uitoefenen. Het bedrijf moet aantoonbaar voldoen aan wet- en regelgeving (accountability). Dit moet ook te controleren zijn door derden (trust but verify uitgangspunt).

Artikel 30 van de AVG wijst organisaties op een documentatieplicht voor het registeren van verwerkingsactiviteiten. Dit register moet beschikbaar zijn voor de toezichthoudende autoriteit. De wet zegt tevens dat alle gegevens die noodzakelijk zijn voor het bieden van transparantie, moeten worden geboden aan de betrokkene.

TNO ziet op technisch vlak dat grotere transparantie in het systeem gecreëerd kan worden door instrumenten aan te bieden die het mogelijk maken bij te houden welke systemen bewerkt worden, door wie en wanneer. TNO noemde in Figuur 5 PET's met betrekking tot transparantie zoals: transparency tools, reputation systems en audit logs.

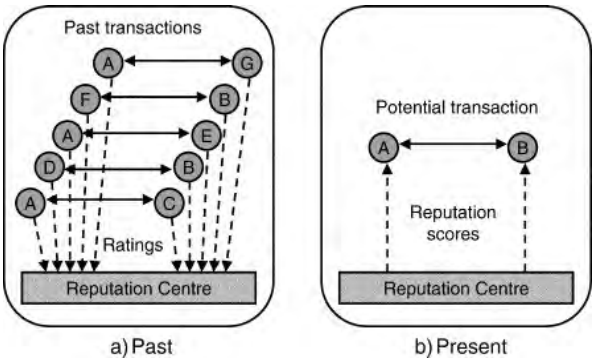
Transparency Tools
TNO ging destijds in 2012 niet verder in op Transparency tools. Echter, in juni 2013 verscheen een artikel 'Transparency Enhancing Tools (TET's): An Overview' van drie TNO medewerkers, waarbij verder ingegaan wordt op Transparency Enhancing Tools. TET's moeten voldoen aan één van de volgende kenmerken:

- Verschaft de gebruiker informatie over de voorgenomen verzameling, opslag, verwerking en/of openbaarmaking van gegevens.
- Verschaft de gebruiker (achteraf) informatie over de verzameling, opslag, verwerking en/of openbaarmaking van gegevens.
- De voorgenoemde punten worden in een accurate, en voor een gemiddelde Internet gebruiker, begrijpelijke manier weergegeven.

Reputation systems

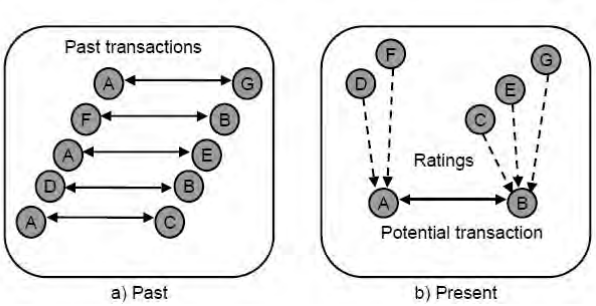
TNO gaat niet verder in op Reputation systems. Bij verder onderzoek geeft Professor Jøsang, verbonden aan de Universiteit van Oslo, in zijn publicatie 'Trust and Reputation Systems' onder andere uitleg over Reputation systems. Bij een Reputation system gaat het in essentie om het mogelijk maken van het beoordelen van partijen, gebruikmakend van de geaggregeerde score van een gegeven partij om daarbij de reputatiescore af te leiden. De reputatiescore kan vervolgens gebruikt worden door andere partijen, bij het besluit om wel of niet in zee te gaan met deze partij. Er bestaan twee hoofdarchitecturen met betrekking tot Reputation systems namelijk gecentraliseerde en gedistribueerde Reputation systems.

Bij gecentraliseerde Reputation systems wordt informatie over de prestatie van een bepaalde partij als een score verzameld van leden van een groep, die met de betreffende partij ervaringen hebben gehad. Een reputation centre verzamelt alle scores en maakt deze publiek beschikbaar zodat andere participanten hiervan gebruik kunnen maken bij in hun besluit om met deze partij in zee te gaan (Figuur 10).



Figuur 10. General framework for a centralised reputation system, uit 'Trust and Reputation Systems' door A. Jøsang, verschenen in A. Aldini and R. Gorrieri (Eds.), Foundations of Security Analysis and Design

Bij gedistribueerde Reputation systems is er geen centrale locatie voor het verzenden en ontvangen van scores over een partij. In plaats daarvan zijn er gedistribueerde locaties waar scores naar toe gezonden kunnen worden of elke participant houdt zijn eigen mening of score bij over de ervaringen met de betrokken partij. Iemand die in zee wil gaan met een bepaalde partij moet dus een gedistribueerde locatie opzoeken of zoveel mogelijk participanten vinden met eerdere ervaringen of scores over de betreffende partij (Figuur 11).



Figuur 11. General framework for a distributed reputation system, uit 'Trust and Reputation Systems' door A. Jøsang, verschenen in A. Aldini and R. Gorrieri (Eds.), Foundations of Security Analysis and Design

Audit logging
Het begrip audit logging wordt niet uiteengezet door TNO. Het National Institute of Standards and Technology geeft in haar publicatie 800-92 aan dat een log een vastlegging is van events die plaatsvinden op systemen en netwerken binnen een organisatie.

Case study

The Global Standard on Privacy by Design van de Rabobank gaat in op: Transparency. De manier waarop Privacy by Design is geïmplementeerd door de Rabobank, het management en de medewerkers zal alle stakeholders verzekeren dat de discussies, assessments en besluiten met betrekking tot data privacy transparant en zichtbaar zijn.

In een aantal werkpakketten van het programma GDPR komen elementen van het principe Transparency and Visibility terug, namelijk in het werkpakket 'Dataretention', waarbij wordt gewerkt aan het opleveren van een verwerkingsregister (met onder andere het doel van de verwerking en de genomen beveiligingsmaatregelen). En daarnaast het werkpakket 'Rights of data subjects', waarin uitwerking plaats vindt van uitgebreide rechten zoals: recht op informatie, recht op toegang, recht op rectificatie, recht om vergeten te worden, recht op beperking van de verwerking en de informatieplicht aangaande rectificatie. Ook het werkpakket 'Accountability' richt zich op transparantie door de verplichting te implementeren waarbij de Rabobank kan aantonen dat zij voldoet aan de GDPR door verplichte documentatie en het opstellen van PIA's bij de implementatie van nieuwe producten, processen, procedures of contracten. Het programma Record Keeping heeft ook een aandeel in dit principe door het opleveren van een Data Retentie register.

De SVB heeft bij de implementatie van de AVG speciale aandacht voor de directe uitwerking op de burger en hecht veel belang aan het register van verwerkingsactiviteiten, de informatieplicht en het inzagerecht.
De SVB is in de meeste gevallen niet verplicht betrokkenen te informeren over het verwerken van hun persoonsgegevens, aangezien artikel 14 een uitzondering maakt voor gegevens waarvan het verkrijgen of verstrekken hiervan is voorgeschreven vanuit de wet.
Ondanks deze uitzondering is in een workshop besproken dat het **niet** informeren van burgers over de verwerking van hun gegevens niet zou aansluiten bij het transparantiebeginsel dat de SVB propageert. Toch bestond er zorg over de vragen die het zou oproepen als alle Nederlanders hierover alsnog een brief zouden ontvangen. Daarom is gekozen voor de middenweg: burgers worden voortaan in de correspondentie bij een eerste beschikking (besluit over toewijzing van een bepaald recht) geïnformeerd over de verwerking van hun persoonsgegevens. Tevens wordt in deze correspondentie verwezen naar de SVB Privacy Portal.

De SVB kiest ervoor om het grootste gedeelte van de geregistreerde verwerkingen in het register op deze website te publiceren.
Voor het in elektronische vorm opstellen van het register zal de SVB gebruik maken van een tool.
Met betrekking tot het inzagerecht en correctierecht is, gezien het beperkte aantal aanvragen dat hiervoor onder de Wbp wordt gedaan, besloten dit op een niet geautomatiseerde wijze uit te voeren.

Visibility and Transparency worden door beide organisatie ingevuld door het opstellen van een verwerkingsregister en door processen om te voldoen aan de rechten van betrokkenen.

5.7 PbD principe 7: Respect for User Privacy – Keep it User-Centric

Het 7e en laatste principe van PbD luidt: Respect for user privacy – keep it user centric. Volgens Ann Cavoukian gaat het hierbij om het centraal stellen van de gebruiker. Dit is mogelijk door passende kennisgeving, het geven van toegang tot informatie over de gebruiker zelf en over de omgang met persoonsgegevens binnen de organisatie.

De wetgeving is in de artikelen 15-21 duidelijk over de rechten die betrokkenen hebben en heeft daarvoor de wettelijke kaders neergelegd in de AVG, zoals de mogelijkheid van betrokkenen om bezwaar aan te tekenen, om hun informatie te wissen, te rectificeren, in te zien, te verhuizen. De invulling van het principe 6 Visibility and Transparency, het bieden van transparantie, is randvoorwaardelijk bij het kunnen uitoefenen van deze rechten.

In elk van de bestudeerde bronnen is duidelijk dat de maatregelen in dienst staan van de bescherming van de persoonlijke levenssfeer van betrokkenen. TNO heeft het over respect voor de individu door betrokkenheid van het datasubject en het expliciet maken van het respect voor de privacy van het datasubject. TNO noemt bij betrokkenheid van het datasubject het fenomeen dat de betrokkene een rol gaat spelen bij de systeemontwikkeling, zodat diens opvattingen meegenomen worden in de ontwerppraktijken.

Het CIP stelt dat Privacy by Design boven alles architecten en exploitanten nodig heeft die de belangen van het individu als hoogste prioriteit beschouwen en dit toepassen door het instellen van krachtige privacy instellingen, passende informatievoorziening en gebruikersvriendelijke opties. Zij stellen de betrokkene te allen tijde centraal. Het credo luidt dan ook: “technische en organisatorische maatregelen zijn pas effectief, wanneer zij de persoonlijke levenssfeer van eenieder beschermen“.

VKA geeft aan dat in de privacywetgeving de bescherming van de persoon centraal staat en dat deze ook is vastgelegd in het Europees Verdrag voor de rechten van de mens. Het grondrecht houdt in dat ieder persoon recht heeft op de eerbiediging van zijn persoonlijke levenssfeer.

Case study

In de Rabobank gedragscode worden vier kernwaarden van de bank genoemd, namelijk respect, integriteit, duurzaamheid en professionaliteit. Ten aanzien van respect werkt de Rabobank samen op basis van respect, waardering en betrokkenheid. Klanten die hun betrokkenheid bij de bank vormgeven in een lidmaatschap verwerven zeggenschap over de koers en de wijze waarop de Rabobank bijdraagt aan het realiseren van hun ambities. In het coöperatieve gedachtengoed kan de betrokkenheid van de klanten worden herkend. Het werkpakket Privacy by Design hanteert het credo van het CIP.

Sinds mei 2016 wordt binnen de SVB gewerkt vanuit ‘de Bedoeling’. De SVB ziet dat bij wijzigingen in wet- en regelgeving niet in alle gevallen de bedoeling tot stand komt. Soms raakt bij het uitvoeren van de wet

naar de letter, de geest van de wet, de bedoeling, verloren en ondervindt de klant daar onterecht nadeel van. Ook de onderwerpen uit de AVG zijn in sessies besproken vanuit 'de Bedoeling' voor burgers. Bescherming, transparantie, zeggenschap en toezicht op betrouwbaarheid zijn hierbij geplot op het eerder genoemde model van de CIP Privacy Baseline (Figuur 4). Hierbij zag de SVB bij de normen 'Register', 'Informatieplicht', 'Bewaren van persoonsgegevens' en 'Inzagerecht', een directe uitwerking voor de burger. Deze normen hebben dan ook extra aandacht gekregen.

De klant is belangrijk! Respect voor de privacy van gebruikers is de uitkomst van de optelsom van PbD principe 1 tot en met 6.

5.8 Conclusie

De 7 Privacy by Design principes van Ann Cavoukian zijn elk conceptueel van aard. Nergens wordt de invulling van de principes duidelijk afgebakend en sommige principes lijken in elkaar over te lopen. Ann Cavoukian gaat ervan uit dat Privacy by Design niet alleen wordt gewaarborgd door het naleven van wet- en regelgeving, maar idealiter besloten ligt in de modus operandi van een organisatie. Niettemin toont zij zich verheugd over het feit dat 'de taal van Privacy by Design' zal worden opgenomen in een nieuwe geharmoniseerde Europese wetgeving in het kader van de bescherming van persoonsgegevens.

Onderdelen uit het concept Privacy by Design zijn in de gehele AVG terug te vinden. Hét Privacy by Design artikel van de AVG, artikel 25, geeft weinig handvatten voor het implementeren van Privacy by Design. De AVG is, net als de Wbp, een beginselenwet. Dat wil zeggen dat er open normen zijn, er staat niet letterlijk in de wet hoe deze normen toegepast moeten worden. Om goed te kunnen voldoen aan de wet, moeten afwegingen gemaakt worden die specifiek van toepassing zijn op betreffende organisaties. Dit geldt ook voor het voldoen aan artikel 25.

In de bestudeerde handreikingen die zijn verschenen in de aanloop naar de AVG is een omslag te merken van een Privacy Enhancing Technology benadering naar een meer systemische benadering (van wieg tot wieg) waarbij ook niet-technische aspecten nadrukkelijk worden betrokken. Hierin wordt de invloed van Ann Cavoukian duidelijk.

De wijze waarop de twee onderzochte organisaties de AVG/GDPR implementeren, vertoont veel overeenkomsten. Er is geen sprake van grote verschillen tussen beide organisaties. De case studies laten zien dat beide organisaties een programma of project hebben opgezet om de implementatie van de AVG, en daarmee Privacy by Design in bredere zin, te realiseren. Dit geldt voor het invullen van randvoorwaarden, zoals beschreven onder Privacy by Design principe 1 en voor specifieke aandachtspunten met betrekking tot de AVG, zoals het aanpassen van het PIA-proces (principe 3) of het opstellen van een verwerkingsregister (principe 6).

Als we ingaan op het écht inbouwen van privacybescherming in het IT-landschap, dan valt op dat óf Privacy by Design maatregelen al in-place waren, zoals bij End-to-End Beveiliging, óf dat voor 25 mei 2018 een opzet geïmplementeerd zal zijn, zoals beschreven onder principe 2 Privacy als Default.

De AVG heeft grote impact op vrijwel alle organisatieonderdelen, zowel op technisch, juridisch als op organisatorisch vlak. Het verdient aanbeveling om Privacy by Design compliance te beoordelen met een audit-team dat is samengesteld uit verschillende audit-disciplines, zoals IT-audit, Operational audit en Compliance audit. De komende jaren zal PbD binnen organisaties verder vorm krijgen en meer volwassen worden. Aanbeveling aan de (interne) IT-auditor, is om, naast het op de voet volgen van de PbD ontwikkelingen

in de markt, ook de discussies binnen de eigen organisatie te kennen. De adviezen en het oordeel van de IT-auditor blijven hierdoor passend voor de organisatie.

6 Literatuurlijst

Boeken

Privacy by Design, F. van Vonderen, Verdonck, Klooster & Associates, juni 2017

Design patterns, elements of reusable object-oriented software, Erich Gamma, Richard Helm, Ralph Johnson en John Vlissides, Addison Wesley, 1995

Privacy Enhancing Technologies - Witboek voor beslissers, Koorn, e.a. 2004

Artikelen

Privacy Design Strategies, Jaap-Henk Hoepman, October 25, 2012 https://www.cs.ru.nl/~jhh/publications/pdp.pdf

Privacy Design Strategies (extended abstract), Jaap-Henk Hoepman, March 14, 2014 https://www.cs.ru.nl/~jhh/publications/pdp-sec.pdf

A Critical Analysis of Privacy Design Strategies, Michael Colesky, Jaap-Henk Hoepman, Christiaan Hillen, 2016 https://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf

Trust and Reputation Systems, A. Jøsang, verschenen in A. Aldini and R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV, FOSAD 2006/2007 Tutorial Lectures. Springer LNCS 4677. Bertinoro, Italy, September 2007 http://folk.uio.no/josang/papers/Jos2007-FOSAD.pdf

How is Positive-Sum Privacy Feasible?, Christoph Bier, Pascal Birnstill, Erik Krempel, Hauke Vagts, Jürgen Beyerer, 7th Security Research Conference 2012. Proceedings : Bonn, Germany, September 4-6, 2012 https://pdfs.semanticscholar.org/1259/df9d2f968d6e97d3aab35cfbf5241e5766f5.pdf

Collegesheets Introduction to privacy & privacy auditing, R. Koorn, september 2016

Geraadpleegde websites

http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN 13-04-2018

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML 13-04-2018

http://wetten.overheid.nl/BWBR0011468/2017-03-10 13-04-2018

http://wetten.overheid.nl/BWBR0007376/2015-07-18 13-04-2018

https://www.rijksoverheid.nl/documenten/rapporten/2012/05/01/stimulerende-en-remmende-factoren-van-privacy-by-design-in-nederland 13-04-2018

https://www.rijksoverheid.nl/documenten/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst 13-04-2018

https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia 13-04-2018

https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf 13-04-2018

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf 13-04-2018

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf 13-04-2018

https://www.cip-overheid.nl/wp-content/uploads/2018/03/20171030-Privacy-Baseline-v3_1.pdf 13-04-2018

https://cip-overheid.nl/wp-content/uploads/2018/03/20170507-Handleiding-Privacygovernance-v3_0.pdf 13-04-2018

https://cip-overheid.nl/wp-content/uploads/2018/03/20170507-Handleiding-Privacy-by-Design-v3_0.pdf 13-04-2018

https://www.socialevraagstukken.nl/driegesprek-rijksincassobeheer-wordt-menselijker-overheid/ 13-04-2018

https://www.surf.nl/binaries/content/assets/surf/en/2013/het-europees-privacyrecht-in-beweging_bw_v2.1.pdf 13-04-2018

https://www.deitauditor.nl/business-en-it/een-nieuw-privacy-control-framework-als-onderdeel-van-de-informatiehuishouding/ 13-04-2018

https://www.norea.nl/download/?id=522 13-04-2018

http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_en.pdf 13-04-2018

https://www.privacycompany.eu/files/Privacy%20by%20Design%20Framework.pdf 13-04-2018

https://www.privacypatterns.org 13-04-2018

https://bauhaus.nl/gdpr-privacy-by-design-in-praktijk/ 13-04-2018

https://www.researchgate.net/publication/260762644_Transparency_Enhancing_Tools_TETs_An_Overview 13-04-2018

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf 13-04-2018

https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf 13-04-2018

https://www.law.berkeley.edu/wp-content/uploads/2016/03/Ann-Cavoukian.pdf 13-04-2018

http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf 13-04-2018

Adoptie data analyse en process mining binnen ADR

Stefanie ten Napel

Stefanie heeft bedrijfskunde gestudeerd aan de EUR, is registeraccountant, en heeft in 2018 de opleiding IT-audit Compliance & Advisory afgerond.
Zij werkt momenteel als Lead IT-Auditor bij de Auditdienst Rijk van het Ministerie van Financiën (ADR), waar zij onder meer betrokken is bij onderzoeken naar GITC en application controls rond SAP en andere kernsystemen, en het toepassen van data-analyse in de audit.
Daarvoor was zij werkzaam bij de interne auditdienst van het Ministerie van Buitenlandse Zaken en in financiële functies bij non-profit organisaties (CARE Nederland, ICCO).

1 Inleiding

De samenleving digitaliseert in een steeds sneller tempo en dit geldt ook voor het werkterrein van financial auditors. Ondernemingen en organisaties gebruiken steeds meer systemen en de hoeveelheid data die dit oplevert, groeit exponentieel. Dit eist van auditors dat deze zelf ook meer gebruik van IT maken in hun werk. Er zijn wat dit betreft hoge verwachtingen van het gebruik van data-analyse en *process mining*, maar het implementeren hiervan blijkt in de praktijk lastig. Dit onderzoek is gericht op de vraag welke belemmerende factoren interne auditdiensten ervaren bij adoptie van deze technieken, met als casus de Auditdienst Rijk.

1.1. Achtergrond en context

Snellere en verdergaande digitalisering van de samenleving stelt nieuwe eisen aan audits

De samenleving digitaliseert in een steeds sneller tempo en deze digitalisering raakt steeds meer aspecten van ons bestaan. Dit biedt mogelijkheden maar leidt het ook tot grote uitdagingen. Ondernemingen en organisaties gebruiken steeds meer systemen en de hoeveelheid data die dit oplevert, groeit exponentieel. Dit stelt nieuwe eisen aan de manier waarop de accountant zijn rol invult. De beroepsgroep is zich bewust van deze uitdaging; digitalisering staat bovenaan het lijstje “ontwikkelingen met impact” in de recent gepubliceerde bestuursvisie van het NBA (2018).

De ADR beweegt richting een *IT-driven* controle-aanpak

Tot 2012 bestonden er binnen de Nederlandse rijksoverheid diverse departementale interne auditdiensten. Als gevolg van een besluit in de Ministerraad zijn deze samengevoegd tot één interne auditdienst voor de gehele rijksoverheid: de Auditdienst Rijk. Om de dienst toekomstbestendig te maken, werd onder meer besloten dat de controleaanpak meer *IT-driven* zou moeten worden.

Inrichting van Analytics Team om het gebruik van IT te bevorderen

Ter bevordering van een *IT-driven* aanpak zijn de afgelopen jaren verschillende initiatieven ontplooid, waaronder het oprichten van een *Analytics*-team dat onder meer als taak heeft om het gebruik van data-analyse en *process mining* in de controle te bevorderen en praktisch te ondersteunen. Een belangrijke activiteit van dit team is het organiseren van zgn. Datathons. Hierbij wordt met een groep financial auditors bij een specifiek ministerie, in korte tijd, aan de hand datasets die voor hun controles relevant zijn, geïdentificeerd welke auditvragen ten aanzien van die data bestaan en hoe deze door middel van data-analyse of *process mining* mogelijk zouden kunnen worden beantwoord. Tijdens de Datathon wordt geprobeerd met het feitelijk beantwoorden van die vragen een start te maken, zodanig dat de financial auditors hier bij hun verdere controlewerkzaamheden direct gebruik van kunnen maken.

Kansen en verwachtingen rond het gebruik van data-analyse en *process mining*

De directie van de ADR ziet kansen dat de audit op de financiële verantwoording van ministeries door een *IT-driven* aanpak efficiënter en effectiever zal kunnen worden uitgevoerd. Uit onder meer de Datathons blijkt echter dat het vlot realiseren van een efficiëntievoordeel in de praktijk om diverse redenen lastig kan zijn. Het gebruik van data-analyse en *process mining* is binnen de ADR nog geen gemeengoed.

Mede gezien het feit dat publieke accountantskantoren in hun marketing-uitingen in toenemende mate aandacht besteden aan digitalisering bij hun klanten, zou de verwachting kunnen zijn dat data-analyse in de publieke controlepraktijk al lang standaardpraktijk is. Dit is echter niet het geval: uit een recent onderzoek van de Britse *Financial Reporting Council* (FRC) blijkt dat *“the use of data analytics in the audit is not as prevalent as the market might expect”* (2017, p. 11). Alhoewel druk gevoeld wordt om data-analyse te

promoten om hiermee tegemoet te komen aan verwachtingen van audit committees, alsmede zich te profileren richting nieuwe klanten, blijkt door de zes grootste Britse accountantskantoren uitsluitend "journal entry testing" breed te worden toegepast.

Het wetenschappelijk onderzoek dat is uitgevoerd naar adoptie van nieuwe audit-technologie biedt aanknopingspunten inzake de voorwaarden waaraan moet worden voldaan voor succesvolle modernisering van de audit. De *Financial Reporting Council* (2017) beschrijft het belang van de uitrol van standaard audit data-analyse *tools* en het beschikbaar maken van specialistische ondersteuning om data te verkrijgen; dit vergroot de kans dat data-analyse succesvol wordt toegepast door controleteams. *Byrnes, Al-Awadhi, Gullvist et al.* (2015, pp. 82-83) verwijzen naar een lijst van zes voorwaarden om audits te moderniseren zoals gepubliceerd door CICA/AICPA in 1999, waaronder (1) een onderzoeksobject met geschikte eigenschappen, (2) audit-*evidence* voortgebracht door in hoge mate geautomatiseerde processen en (3) een hoge mate van bekwaamheid van de auditor in zowel IT als het onderzoeksobject. Byrnes, Al-Awadi, Gullvist et al. merken m.b.t. verschillende van de zes voorwaarden op dat hieraan nog niet of pas recent is voldaan, of dat aandacht voor het betreffende punt in de audit nog beperkt is. De auteurs stellen m.b.t. het realiseren van de voordelen van een gemoderniseerde audit: *"Although the system architecture and software components are extremely important considerations, complementary elements such as auditor education, the socio-technical environment of the firm, and tone at the top are fundamental as well."*

Byrnes, Al-Awadi, Gullvist et al. concluderen bovendien: *"Consequently, comprehensive strategic planning that joins technical issues with human issues is also a necessary ingredient in helping to ensure a successful transition to the future audit."* (Byrnes, Al-Awadi, Gullvist et al., 2015:83). Dit laatste – een uitgebreid, integraal strategisch plan voor invoering van de 'audit van de toekomst' – is als zodanig door de ADR (nog) niet opgesteld.

1.2. Vraagstelling

Gezien de noodzaak voor accountants om meer gebruik van IT te maken in de audit, en de observatie dat het gebruik van data-analyse en *process mining* bij de ADR in de praktijk nog geen hoge vlucht heeft genomen, luidt de onderzoeksvraag:

> *Welke belemmerende factoren ervaren interne auditdiensten bij de adoptie van het gebruik van IT bij de audit, in het bijzonder data-analyse & process mining, en welke maatregelen kunnen bijdragen aan het verminderen of wegnemen van deze belemmeringen?*

met als deelvragen:

1 Wat wordt verstaan onder data-analyse en process mining als voorbeelden van gebruik van IT in de audit?
2 Welke belemmerende factoren kunnen er bestaan m.b.t. adoptie van het gebruik van IT in de audit, en in welke mate vormen deze factoren een belemmering bij het adoptieproces van data-analyse en process mining?
3 Welke maatregelen kunnen interne auditdiensten nemen om deze belemmeringen te mitigeren of weg te nemen en hun dienstverlening verder te moderniseren?

2 Theoretisch kader

2.1 Het auditproces

In de essentie draait het bij een auditproces altijd om het toetsen van de werkelijkheid aan een norm. In de loop van de tijd zijn er echter veel ontwikkelingen geweest in *scope*, diepgang en aanpak van audits. Het

gebruik van IT in brede zin, en van bepaalde technieken in het bijzonder, is een meer recente ontwikkeling. De verwachting is dat IT in de audit van de toekomst een nog veel grotere rol zal spelen.

2.1.1 De definitie van een audit

Voor financial auditors staat een audit over het algemeen synoniem aan een assurance-onderzoek: een opdracht waarbij zekerheid wordt verschaft bij financiële overzichten. Hierbij toetst de accountant de door een klant opgestelde financiële overzichten aan normen voor financiële administratie en presentatie. Doel is om vast te stellen of deze een getrouw beeld geven van financiële stromen en balansposities, zodat een gebruiker ervan beslissingen kan nemen op basis van betrouwbare informatie. De wijze waarop een auditor dergelijk onderzoeken moet uitvoeren, ligt vast in vaktechnische standaarden die internationaal worden bepaald door het IFAC (International Federation of Accountants). In Nederland moeten auditors voldoen aan de eisen van de Handleiding Regelgeving Accountancy van de Nederlandse Beroepsorganisatie van Accountants (NBA) – de hierin opgenomen NV COS zijn grotendeels identiek aan de internationale standaarden.

2.1.2 Evolutie van de audit in de loop van de tijd

De geschiedenis van de financial audit gaat in Nederland terug tot omstreeks 1900. Sindsdien zijn er belangrijke veranderingen geweest in de manier waarop een audit wordt uitgevoerd. Gonsalves Jardin de Ponte (2010, pp. 6-8) schetst hoe accountantscontrole ontstond als vorm van administratieve bijstand aan ondernemingen. In de eerste helft van de vorige eeuw waren integrale controle (van alle bewijsstukken) en later de zgn. “volkomen controle” van Limperg (gebaseerd op omspannende verbandcontroles) de norm. In de tweede helft van de 20e eeuw groeit de aandacht voor interne controle binnen bedrijven en de vraag in hoeverre de accountant hierop mag steunen; zo ontstaat een verschuiving van volledig gegevensgerichte controle naar een deels systeemgerichte controle: als de accountant kan vaststellen dat een administratief systeem betrouwbaar en nauwkeurig werkt, hoeven minder individuele gegevens gecontroleerd te worden. Vanaf 1988 neemt de aandacht voor risicoanalyse toe, waarbij de accountant zijn (systeemgerichte) werkzaamheden met name richt op die posten en stromen in de jaarrekening waar het grootste risico bestaat op een afwijking van materieel belang.

2.1.3 Het gebruik van IT en de audit van de toekomst

Ook het object van onderzoek heeft een evolutie doorgemaakt. Byrnes, P., Al-Awadhi, A., Gullvist, B., & et al. (2015) vermelden dat halverwege de 20e eeuw de eerste computers verschijnen waarop enige vorm van elektronische boekhouding kan plaatsvinden. Het belang van computers binnen de bedrijfsadministratie heeft sindsdien een hoge vlucht genomen. Roos Lindgreen (2016) beschrijft hoe in reactie hierop in de jaren 70 het vak van Electronic Data Processing (EDP) auditor ontstond, om vast te stellen of de door bedrijven gebruikte informatiesystemen voldoende betrouwbaar waren om de uitkomsten ervan in de audit te kunnen gebruiken. Volgens Roos Lindgreen was de uitkomst van deze audits vaak teleurstellend. Ofwel de General IT Controls, ofwel de application controls bleken niet aan de eisen te voldoen, zodat de accountant moest terugvallen op het uitvoeren van meer gegevensgerichte werkzaamheden. De steeds snellere technologische ontwikkelingen maken het werk van de EDP-auditor (tegenwoordig: IT-auditor) er niet makkelijker op. De prilste informatiesystemen waren autonome, afgegrensde en daardoor overzichtelijke eenheden, maar dit veranderde al sterk met de komst van internet, laptops en het uitbesteden door bedrijven van IT-werkzaamheden aan onderaannemers. Roos Lindgreen gebruikt in relatie tot de ontwikkelingen uit de laatste 10 jaar zoals smartphones, cloud en wearables het woord “tsunami” voor de toename van alle verschillende software die in verbinding staan met informatiesystemen en deze kwetsbaar kunnen maken. Hij stelt dat het onder deze omstandigheden moeilijker dan tevoren en soms zelfs onmogelijk is, om vast te stellen dat een informatiesysteem gedurende 12 maanden (de periode waarop financial audits vaak betrekking hebben) op betrouwbare wijze heeft gefunctioneerd. De auditor zal daarom terug moeten vallen op gegevensgerichte controle, maar kan daarbij in tegenstelling tot vroeger gebruik maken van IT om

deze werkzaamheden te automatiseren en sneller grotere hoeveelheden data te controleren. Byrnes, P., Al-Awadhi, A., Gullvist, B., & et al. (2015) merken op dat de efficiëntie en effectiviteit van de audit hierdoor aanzienlijk vergroot worden. Zij zien het gebruik van zgn. computer-assisted audit tools & techniques (CAATTs) als een tussenstap naar continuous auditing: het real time en vrijwel volledig geautomatiseerd controleren van alle datastromen in de bedrijfsadministratie.

2.2 Data-analyse en process mining

Het gebruik van IT binnen de audit kent vele verschijningsvormen, en sommige zgn. *Computer-Assisted Audit Tools* & *Techniques* (CAATTs) worden al heel lang toegepast. Wat wordt in dit kader verstaan onder data-analyse en *process mining?*

2.2.1 Computer-Assisted Audit Tools & Techniques

Stewart (2015, p. 105) gebruikt de term data analytics om de wetenschap aan te duiden die zich bezighoudt met "het ontdekken en analyseren van patronen, het identificeren van afwijkingen en het onttrekken van andere nuttige informatie uit data onderliggend of gerelateerd aan het audit-object, door analyse, modellering en visualisatie ten behoeve van het plannen of uitvoeren van de audit". Hij benadrukt daarbij dat auditors dit altijd al deden; technologie heeft de manier verbeterd waarop dit gebeurt, maar het proces is hetzelfde gebleven. Data analytics kunnen worden toegepast in elke fase van de audit (planning, verkrijgen van inzicht in een entiteit, inschatten van het risico op een afwijking van materiaal belang, testen van interne controls en uitvoeren van gegevensgerichte werkzaamheden).

Bij een brede definitie van CAATTs gaat het volgens Braun & Davis (2003, p. 726) om "elk gebruik van technology bij het uitvoeren van een audit". Hierbij merken zij op dat de meeste definities CAATTs uitsluitend gebruiken om tools en technieken aan te duiden die worden gebruikt danwel voor de audit van computertoepassingen, danwel voor het extraheren en analyseren van data. Daarmee kunnen CAATTs gezien worden als een technische invulling van data analytics.

Ook met deze nadere toespitsing omvat de term CAATTs een zeer grote verscheidenheid aan toepassingen en applicaties, variërend van breed bekende en laagdrempelige uit de Microsoft Office Suite zoals Excel tot allerlei minder bekende pakketten met meer specialistische functionaliteit. De website www.softwareadvice.com noemt in mei 2018 alleen in de categorie voor business intelligence al 161 applicaties. Kunnen omgaan met een meer specialistische CAATT vraagt een tijdsinvestering; het ligt daarom voor de hand dat het aantal verschillende meer specialistische CAATTs binnen één accountantsorganisatie beperkt is.

2.2.2 Data-analyse

Zoals beschreven in de voorgaande sectie 2.2.1, heeft de term data analytics of data-analyse betrekking op een breed scala aan activiteiten om informatie te ontlenen aan data ten behoeve van de audit. Er is veel onderzoek uitgevoerd naar de toepassing hiervan. Appelbaum, Kogan & Vasarhelyi (2018) hebben ruim 300 online toegankelijke artikelen geïdentificeerd, gepubliceerd in de periode 1965-2015, die betrekking hebben op data-analyse in relatie tot (enige fase van) de externe audit. Uit hun analyse blijkt dat de fases van risicoanalyse, audit-planning en gegevensgerichte werkzaamheden het meest onderzocht zijn; deze komen voor in 75% van de artikelen. De reviewfase komt in ruim de helft van de artikelen aan de orde. Toepassing van data-analyse bij het begin van de audit (klant-acceptatie) of het einde (rapportering) wordt slechts in respectievelijk 12% en 15% van de papers behandeld.

Van de door Appelbaum, Kogan & Vasarhelyi gehanteerde categorieën van data-analyse-technieken, is de groep "audit examinations" veruit dominant. Hiertoe behoren onder meer ratio-analyse, het trekken van steekproeven en software zoals IDEA die bepaalde auditwerkzaamheden (zoals het trekken van steekproe-

ven) automatiseert. Een tweede, wat minder frequent onderzochte categorie van technieken is “regression”; deze bevat allerlei soorten statistische analyses. Het minst onderzocht is de categorie “unsupervised”, die betrekking op technieken die informatie genereren uit zogenaamde ongelabelde datasets, bijvoorbeeld door middel van clustering of visualisatie.

2.2.3 Process mining

Process mining is gebaseerd op analyse en visuele weergave van zogenaamde event logs. Deze bevatten de vastlegging van gebeurtenissen (events) in computersystemen inclusief de tijdstippen waarop die events plaatsvonden en identificatie van de personen/machines die deze events initieerden of uitvoerden.

Naar aard kan process mining gepositioneerd worden onder de paraplu van business intelligence (Aalst, 2016, pp. 20, 49). Van der Aalst benadrukt echter dat waar business intelligence applicaties de focus leggen bij het opvragen en rapporteren van data in relatief eenvoudige visuele weergaven (dashboards, scorecards), process mining bij uitstek geschikt is voor het inzichtelijk maken van het dynamische gedrag van data. Process mining is vergelijkbaar met data mining, in de zin dat in beide gevallen grote databestanden worden geanalyseerd om onverwachte verbanden te vinden en nieuwe inzichten te genereren. Volgens Van der Aalst (2016, p. 46) is het verschil echter dat de gangbare data-mining technieken in tegenstelling tot process mining de focus niet hebben liggen op processen.

Process mining is breed inzetbaar voor prestatiemeting, het signaleren van afwijkingen, het voorspellen van vertragingen, ondersteunen van besluitvorming en herinrichting van processen. Binnen Financial Audit kan process mining bijvoorbeeld gebruikt worden om vast te stellen of de feitelijk doorlopen processtappen en functiescheiding overeenstemmen met de AO. Een Operational Auditor kan process mining inzetten bij efficiëntie-vraagstukken. Een IT-auditor tenslotte zou met behulp van process mining kunnen nagaan of business rules correct zijn verwerkt in een applicatie.

2.3 Adoptie van nieuwe technologie

De geschiedenis leert dat het geruime tijd kan duren voordat nieuwe technologie breed wordt toegepast. Uit de literatuur blijkt dat dit zeker ook geldt voor het gebruik van IT in de audit. Er bestaan diverse modellen die de mate van acceptatie en gebruik van nieuwe technologie helpen te beschrijven en te verklaren.

2.3.1 Achterblijvend gebruik van IT in de audit

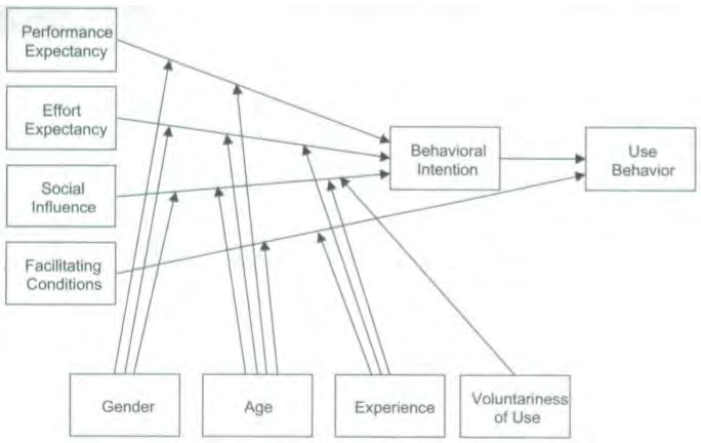
Het in §2.2.2 genoemde aantal onderzoeken naar het gebruik van data-analyse in de externe audit en de hierbij ingezette CAATTs, kan de indruk wekken dat IT ook al veelvuldig bij de audit wordt ingezet. Zoals genoemd in de inleiding, blijkt dit niet het geval. Onderzoek van de Britse Financial Reporting Council wijst uit dat “the use of data analytics in the audit is not as prevalent as the market might expect” (2017, p. 11). Door de zes grootste Britse accountantskantoren uitsluitend “journal entry testing” breed te worden toegepast (Financial Reporting Council, 2017, p. 12). Byrnes, Ames en Vasarhelyi (2015, pp. 54-55) deden eerder al onderzoek naar continuous auditing en concludeerden toen dat dit door grote kantoren nauwelijks wordt toegepast. Uit een recente survey door Protiviti onder meer dan 1500 internal auditors blijkt dat ook zij worstelen met het ontwikkelen van een methodologie om data analytics in hun werk te integreren (Protiviti, 2018).

2.3.2 Wetenschappelijke modellen voor acceptatie en gebruik van technologie

Er zijn in de loop van de tijd veel verschillende modellen ontwikkeld om de mate van acceptatie en gebruik van technologie te verklaren. Een belangrijke bijdrage aan dit onderzoeksveld is geleverd door Venkatesh, Morris en Davis & Davis (2003). Zij analyseerden acht gangbare modellen en formuleerden op basis daarvan het UTAUT-model (Unified Theory of Acceptance and Use of Technology).

Volgens dit model is het gebruik van nieuwe technologie direct afhankelijk van gebruiksintentie en faciliterende omstandigheden. De gebruiksintentie op haar beurt is afhankelijk van verwachtingen m.b.t. prestaties en inspanning en sociale beïnvloeding. Aspecten als geslacht, leeftijd, ervaring en de vraag of gebruik van technologie al dan niet vrijwillig is, zijn van invloed op de kracht van deze afhankelijkheden en worden daarom modererende variabelen genoemd.

Het UTAUT-model is in de afgelopen 15 jaar veel toegepast in onderzoek naar technologie-adoptie, en er zijn variaties op het model ontstaan doordat verschillende onderzoekers aanpassingen of uitbreidingen hebben voorgesteld om het model vollediger te maken.



Figuur 2.1 UTAUT-model

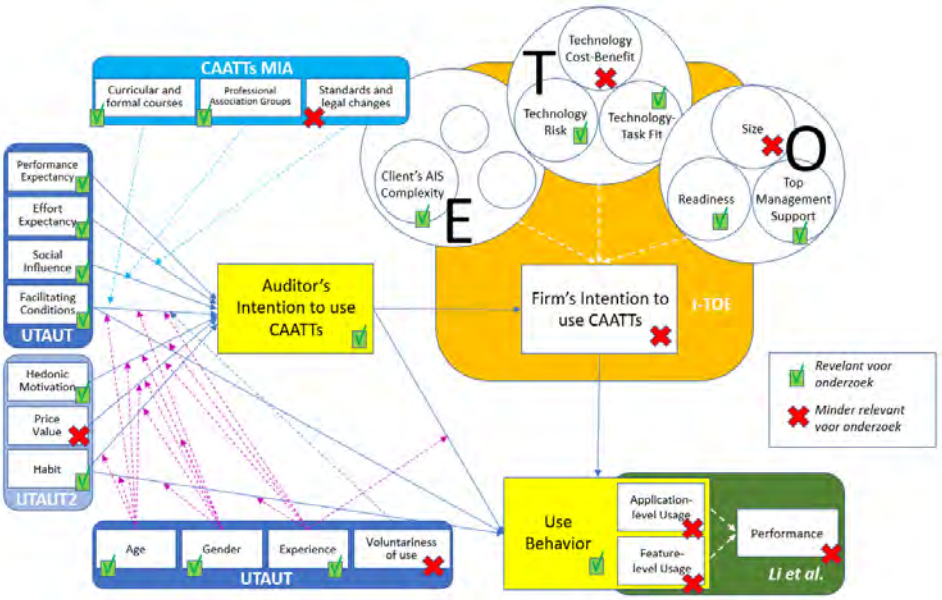
Op het terrein van acceptatie van CAATTs binnen de audit wordt onderzoek gedaan op basis van (gemodificeerde) UTAUT-modellen. Pedrosa en Costa (2011) onderzochten de acceptatie van CAATTs door internal auditors in Portugal en voegen voor hun CAATTs MIA-model *(Model for Individual Acceptance*) drie modererende variabelen toe aan het oorspronkelijke UTAUT-model: training, de invloed van beroepsverenigingen en de impact van standaarden en wet- en regelgeving.

Venkatesh, Thong en Xu (2012) ontwikkelden een tweede versie van het UTAUT-model, UTAUT 2, waarin als nieuwe begrippen gebruiksplezier, financiële kosten/baten en gewoonte worden geïntroduceerd. *Rosli, Yeow* en *Siew* (2012) includeren twee van deze drie aspecten expliciet in hun onderzoek naar technologie-acceptatie door accountantskantoren. Rosli et al. duiden gebruiksplezier als het positieve gevoel dat een accountant zou kunnen ontlenen aan het gebruik van CAATTs (*"using CAATTs in audit work is 'cool' (...) ")* en noemen de kosten/baten van het gebruik van CAATTs als directe factor van invloed op de gebruiksintentie van het accountantskantoor.

Een belangrijk verschil in invalshoek in het werk van Rosli, Yeow en Siew is dat zij de gebruiksintentie van auditor als individu en de gebruiksintentie van de accountantsorganisatie in samenhang bestuderen, vanuit de gedachte dat geen van beiden op zichzelf doorslaggevend is als verklaring voor het gebruik van CAATTs. In hun *I-TOE framework* combineren zij de factoren uit het UTAUT2-model die van invloed zijn op de individuele (I) gebruiksintentie, met technologische (T), organisatorische (O) en omgevingsfactoren (E) die van invloed zijn op de gebruiksintentie van de accountantsorganisatie.

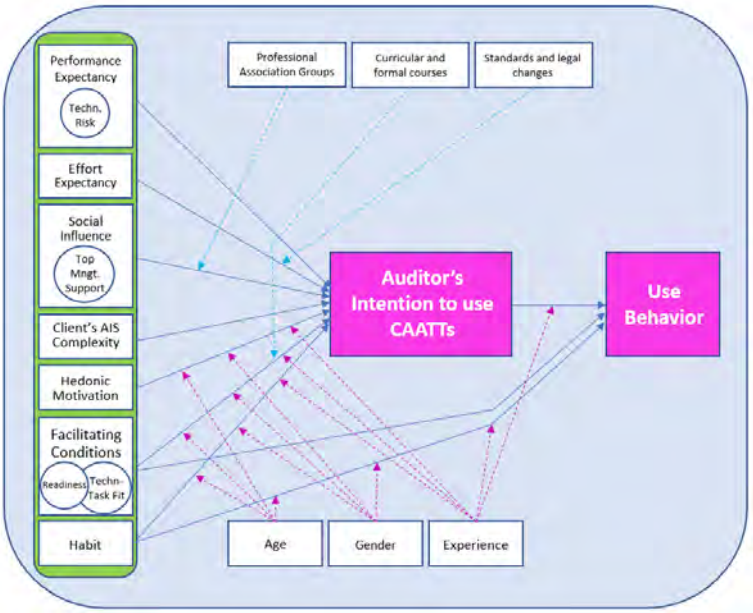
2.4 Onderzoeksmodel

De bestaande wetenschappelijke modellen voor het beschrijven en verklaren van de mate van acceptatie en gebruik van nieuwe technologie in de audit, zoals behandeld in §2.4.2, bieden tezamen een goed overzicht van de verschillende factoren die hierbij van belang kunnen zijn. Tegelijkertijd lijkt niet elk van deze factoren even relevant voor een interne overheidsaccountant. Bovendien is sprake van enige overlap tussen de factoren die in de verschillende modellen genoemd worden. In de onderstaande figuur zijn UTAUT, UTAUT2, CAATTs MIA, I-TOE en het TOE-model van Li et al. samengebracht. Met betrekking tot de verschillende factoren is aangegeven of deze relevant of minder relevant worden geacht voor het onderzoek dat in dit artikel wordt beschreven, gericht op het identificeren van belemmerende factoren voor het gebruik van IT bij de audit, gericht op en door middel van onderzoek onder *medewerkers van een interne auditdienst*.



Figuur 2.2 Totstandkoming onderzoeksmodel

De gemaakte selectie is getoetst in twee workshops met functionarissen vanuit de Auditdienst Rijk (zie § 3.3) en dit heeft geleid tot enkele kleine aanpassingen en het onderstaande definitieve onderzoeksmodel:



Figuur 2.3 Definitief onderzoeksmodel

3 Case-study: bevindingen, analyse en conclusies

3.1 Inleiding

Het onderzoek dat aan dit artikel ten grondslag ligt, bestaat uit een case-study in twee stappen: het houden van expert-interviews in de vorm van workshops met projectleiders en tekenend accountants (stap 1), en een brede survey onder medewerkers (stap 2). Het object van onderzoek binnen de case-study is de Auditdienst Rijk.

3.2 Wat is de Auditdienst Rijk?

Zoals vermeld in de inleiding van dit artikel, is de Auditdienst Rijk (ADR) in 2012 tot stand gekomen via het samenvoegen van diverse departementale auditdiensten, die elk een of meerdere ministeries bedienden. De taken en verantwoordelijkheden van de ADR zijn wettelijk verankerd in de Comptabiliteitswet 2016 en het Besluit Auditdienst Rijk van 19 juni 2018. Hierin is bepaald dat de ADR belast is met de interne auditfunctie bij het Rijk, bestaande uit het uitvoeren van onderzoeken naar en het uitbrengen van een controleverklaring bij de jaarverslagen van de ministeries (de "wettelijke taak") en overige werkzaamheden zoals genoemd in het Besluit Auditdienst Rijk. Daarbij gaat het om onderzoeken die de ADR *op verzoek* kan uitvoeren bij een ministerie of agentschap, of bij organisaties die niet tot de Rijksoverheid behoren (bijv. ontvangers van subsidies of organisaties die zelf een wettelijke taak uitvoeren). Elke minister kan zelf prioriteiten stellen met betrekking tot dit soort ("vraag-gestuurde") onderzoeken. In de Comptabiliteitswet 2016 is tevens vastgelegd dat de Algemene Rekenkamer gebruik kan maken van de werkzaamheden van de ADR.

De ADR is geplaatst binnen het Ministerie van Financiën en heeft een aantal bijzondere kenmerken, waaronder departementale lijnen van opdrachtgeverschap en rapportering. Dit betekent dat de ADR zijn taken uitvoert in opdracht van de individuele ministers en uitsluitend aan hen rapporteert. Daarnaast is bepaald dat de ADR onafhankelijk is in het aanvaarden, uitvoeren en rapporteren over onderzoeken. De ADR wordt periodiek getoetst op kwaliteit door het samenwerkingsverband KOA (Kwaliteitstoets Overheids Auditors)

dat is geaccrediteerd door het NBA, IIA en NOREA. Deze drie beroepsorganisaties vertegenwoordigen de drie audit-disciplines die binnen de ADR actief zijn: *financial* auditors, *operational* auditors en *IT*-auditors. Hoewel deze vakgebieden binnen de ADR organisatorisch zijn ondergebracht in afzonderlijke sectoren, wordt er bij de diverse opdrachten voor de ministeries met regelmaat samengewerkt in multidisciplinaire teams. In totaal zijn bij de ADR ruim 600 auditors werkzaam. Hiervan is 58% actief als financial auditor, 23% als operational auditor en 19% als IT-auditor.

De ADR investeert in het vernieuwen van de gehanteerde controleaanpak. Een van de speerpunten daarbij is het verder ontwikkelen van een *IT-driven* aanpak die aansluit bij de ontwikkelingen op IT-gebied binnen de Rijksoverheid. Een belangrijke rol hierin ligt bij het *Analytics*-team. Een van hun activiteiten bestaat uit het organiseren van de in de inleiding van dit artikel genoemde Datathons. Daarnaast wordt geïnvesteerd in het centraal uitvoeren van transactionele analyses op de grote ERP-systemen die binnen de Rijksoverheid gebruikt worden, en het uitvoeren van kwetsbaarheden-scans. Resultaten van analyses en geëxtraheerde databestanden worden voor bij een specifiek onderzoek betrokken ADR-collega's toegankelijk gemaakt in een speciale *Analytics*-omgeving. In deze omgeving is ook *tooling* beschikbaar voor verdere analyse. Tenslotte wordt ingezet op het gebruik van *data science* en *machine learning*-technieken.

3.3 Workshops: stap 1

Ten behoeve van het vergaren van inzichten met betrekking tot de centrale vraagstelling van dit artikel, en het toetsen van een concept-onderzoeksmodel op juistheid en volledigheid van de geselecteerde elementen, zijn twee workshops gehouden. Deelnemers werden uitgenodigd om de participeren op basis van hun ervaring of affiniteit met data-analyse en/of *process mining*. In totaal namen 13 collega's deel vanuit vijf afdelingen van de ADR.

Tijdens de workshops hebben deelnemers op verschillende manieren het relatieve belang gescoord van de elementen uit het onderzoeksmodel. Uit de toegekende scores blijkt dat men vooral belemmeringen ziet op het terrein van de prestatie- en inspanningsverwachting. De aspecten sociale beïnvloeding en gebruiksplezier worden vrij uniform als weinig belangrijk zien. De aspecten gewoonte, faciliterende omstandigheden en complexiteit van informatiesystemen vormen een middengroep.

Uit tijdens de workshops gevoerde de groepsdiscussie komen de volgende aandachtspunten naar voren:

Prestatieverwachting:
Als belemmerende factor wordt genoemd dat tooling voor het uitvoeren van bepaalde audits niet of minder goed bruikbaar is, bijvoorbeeld bij veel kwalitatieve informatie die van belang is bij prestatievaststelling/rechtmatigheidscontroles. Bij dergelijke audits is tooling hoogstens een extra hulpmiddel. Ook als wel tooling ingezet wordt, moet gekeken blijven worden naar het totstandkomingsproces van data of brondocumenten. Voor specifieke audits kan tooling goede resultaten opleveren, mede omdat door inzet hiervan de inspanning meer specifiek kan worden gericht op bepaalde processen, financiële stromen of transacties met hoger risico. De kwaliteit van de audit kan daardoor toenemen, maar dit geldt niet automatisch ook voor de efficiëntie: het is mogelijk dat inzet van tooling juist extra werk veroorzaakt omdat nieuwe inzichten ontstaan.

Inspanningsverwachting:
Als belemmering wordt de initiële tijdsinvestering genoemd, die nodig is om tooling te implementeren. Op de korte termijn zijn de kosten daardoor waarschijnlijk hoger dan de opbrengsten. En ook op de langere termijn blijft het nodig om tijd te investeren, om te zorgen dat een tool in continuïteit goed blijft werken. De combinatie met hoge werkdruk kan ervoor zorgen dat collega's die benodigde investering

niet kunnen of willen maken. Het centraal aanbieden van bepaalde analyses – ook wanneer die analyses zelf niet heel vernieuwend zijn – betekent een tijdbesparing voor individuele auditors.

Gewoonte:
Mede vanwege de benodigde tijdsinvestering, voelt het voor sommige collega's 'veiliger' om vast te houden aan werkwijzen waarmee men vanuit het verleden vertrouwd is. Soms speelt dit zodanig dat er bij inzet van tooling dubbel werk gedaan wordt, omdat daarnaast ook aan de oude werkwijze vastgehouden wordt. Er speelt onzekerheid mee, of met de nieuwe aanpak de controledoelstellingen wel bereikt worden (betrouwbaarheid brondata, 95% betrouwbaarheid).

Faciliterende omstandigheden:
Als mogelijk belemmerde factor wordt (gebrek aan) beschikbare tijd genoemd. Een ander belangrijk aspect is gebrek aan kennis van de mogelijkheden, bijvoorbeeld met betrekking tot analyses die centraal al beschikbaar zijn. Interactie met IT-collega's en data-analisten is essentieel om een tool goed te kunnen benutten. Wanneer bij een bepaalde groep collega's belangstelling is om tooling toe te passen, is het belangrijk om het momentum vast te houden: "niet kunnen leveren" werkt remmend. Bij sommige tools is specifieke training nodig, en frequent gebruik van de tool om de opgebouwde kennis niet meteen weer te verliezen. De hoge kosten van een tool, en een daardoor laag aantal licenties, kunnen soms ook een belemmering vormen.

Complexiteit van informatiesystemen:
Niet zozeer de complexiteit van de informatiesystemen werkt belemmerend, als wel de beperkte mate waarin sommige informatie hierin (op de juiste manier) is vastgelegd. Een andere factor is het van de klant verkrijgen van data in een gestructureerde en bruikbare vorm. Hierbij speelt mee dat elke klant een eigen data-model hanteert, ook al gebruikt men misschien hetzelfde ERP-systeem. De data van sommige onderzoeksobjecten zijn naar aard minder geschikt om met tooling te bekijken dan andere; processen die primair georganiseerd zijn rond kwantitatieve gegevens leveren veel bruikbaarder data op dan processen met veel kwalitatieve data. In sommige gevallen is sprake van een keten van niet altijd gekoppelde systemen. Het uitvoeren van een analyse over de hele keten is vaak nog niet mogelijk.

Sociale beïnvloeding:
Het bestaan of de afwezigheid van sociale beïnvloeding wordt niet als een factor van belang gezien. Collega's worden niet aangesproken op hun (gebrek aan) gebruik van tooling; individuele accountants zijn zelf verantwoordelijk voor de gekozen controleaanpak. Wel wordt de mening van Algemene Rekenkamer ten aanzien van tooling genoemd als iets waarmee bij de inzet hiervan rekening wordt gehouden.

Gebruiksplezier:
Positieve gevoelens die het gebruik van tooling teweeg zou kunnen brengen worden door de deelnemers niet gezien als iets dat een beslissing over de inzet ervan beïnvloedt.

3.4 Brede survey: stap 2

Als tweede stap in het onderzoek is een brede survey uitgevoerd onder een zo groot mogelijke groep ADR-medewerkers. Er is bewust voor gekozen om niet alleen financial auditors maar ook operational en IT-auditors aan te schrijven, omdat data-analyse en process mining in beginsel in elk van deze disciplines toepasbaar is. Het aantal potentiële respondenten bedroeg daarmee omstreeks 600 collega's. De respons op de survey bestond uit 172 bruikbare enquêtes. De samenstelling van de groep respondenten vormt een redelijk goede doorsnede van de populatie. Alle leeftijdscategorieën zijn ruim vertegenwoordigd met iets hogere respons onder oudere medewerkers, de verdeling man/vrouw bedraagt 77% versus 23% en voor wat betreft audit-discipline is 52% van de respondenten met name actief binnen de financial audit, en 24%

binnen elk van de twee andere disciplines: IT-audit en operational audit. Deze percentages sluiten goed aan bij de opbouw van de ADR (zie § 3.2). Aanvullend is aan respondenten gevraagd wat hun rol binnen het team is. 57% van de respondenten is (deel)projectleider en 35% is teamlid. De resterende 8% vervult beide rollen afwisselend, of is meer indirect bij audits betrokken als data-specialist, coördinator of account-directeur. Respondenten hebben de afgelopen twee jaar audits verricht bij negen verschillende departement(s-onderdel)en.

De groep respondenten heeft duidelijk meer ervaring met data-analyse dan met process mining. Data-analyse is door 69% van de respondenten weleens gebruikt. Van alle respondenten heeft 34% hier vier of meer jaar ervaring mee. Process mining daarentegen is door slechts 33% van de respondenten weleens ingezet, en maar 7% heeft vier of meer jaar ervaring.

Met betrekking tot gebruiksintentie is aan respondenten gevraagd om aan te geven hoe vaak men verwacht data-analyse en process mining over twee jaar te zullen toepassen, vergeleken met het huidige gebruik. Van de respondenten die aangeven een zekere mate van ervaring te hebben met data-analyse of met process mining, geeft twee-derde aan te verwachten dit over twee jaar vaker dan nu toe te passen. Hierbij is men licht positiever over de toepassing van data-analyse. Slechts een klein deel van de respondenten verwacht deze werkwijzen minder vaak toe te zullen passen dan men momenteel doet. Van de respondenten die noch met data-analyse, noch met process mining ervaring hebben, geeft een belangrijk deel aan te verwachten deze werkwijzen ook over twee jaar niet te zullen toepassen.

Gemiddelde score per aspect		
	gewogen gemiddelde	ranking
A011.. Performance Expectancy m.b.t. data-analyse	3,60	1
A012.. Performance Expectancy m.b.t *process mining*	3,51	2
A021.. Effort Expectancy m.b.t. data-analyse	2,61	9
A022.. Effort Expectancy m.b.t. *process mining*	2,59	10
A03 Social Influence	3,47	3
A041.. AIS Complexity m.b.t. data-analyse	3,40	4
A042.. AIS Complexity m.b.t. *process mining*	3,17	6
A05 Hedonic Motivation	3,34	5
A06 Facilitating Conditions	3,11	7
A07 Habit	2,96	8

Tabel 3.1 Gewogen gemiddelde antwoordwaarde en rangorde van aspecten

De voorgelegde survey bestaat voor het grootste deel uit stellingen bij de aspecten uit het onderzoeksmodel, waarbij aan respondenten is gevraagd aan te geven in welke mate men het met de stelling eens of oneens is.
Op basis van een analyse van de gewogen gemiddeldes per aspect, blijkt dat respondenten het - gemiddeld genomen - het meest frequent eens zijn met stellingen die een positieve waardering uitdrukken met betrekking tot aspecten als prestatieverwachting (zowel m.b.t. data-analyse (positie 1) als process mining (positie 2)), en sociale beïnvloeding (positie 3). Op stellingen met een positieve waardering inzake complexiteit van informatiesystemen (positie 4 en 6) en gebruiksplezier (positie 5) reageren de respondenten iets minder vaak instemmend. De laagste gemiddelde waarden hebben betrekking op faciliterende omstandigheden (positie 7), gewoonte (positie 8) en de inspanningsverwachting, zowel met betrekking tot data-analyse als process mining (respectievelijk positie 9 en 10). Hierbij valt op dat de gemiddelde waarden

voor inspanningsverwachting ook duidelijk lager zijn dan 3 (het getal dat correspondeert met een neutrale reactie op de stelling). De gemeten verschillen zijn statistisch significant.

Analoog aan de studie van Venkatesh et al uit 2003 en 2012 is op de via de survey verkregen data een regressie-analyse uitgevoerd. Een dergelijke analyse geeft inzicht in de mate waarin de waarde van een afhankelijke variabele wordt verklaard vanuit een of meerdere onafhankelijke variabelen. De data hebben echter niet tot verklarend model geleid waarbij zowel het model zelf als de componenten ervan statistisch significant zijn, en ook sprake is van een hoge verklarende waarde.

3.5 Antwoorden op open vragen

De survey die aan ADR-collega's werd voorgelegd, sloot af met enkele facultatieve open vragen, waarvan de belangrijkste twee hier behandeld worden. Veel respondenten hebben van deze gelegenheid gebruik gemaakt om hun observaties, zorgen en aandachtspunten over het gebruik van data-analyse en process mining te delen. Reacties zijn zoveel mogelijk gerangschikt naar de zeven aspecten uit het onderzoeksmodel.

3.5.1 Grootste belemmerde factor om gebruik van tooling te vergroten

De eerste open vraag waarop respondenten konden reageren, was: "Wat zie jij als de grootste belemmerende factor om het gebruik van data-analyse en process mining binnen de ADR te vergroten?" Hier gaf 79% (n=143) van de respondenten een antwoord op.

Faciliterende omstandigheden

Een opvallend groot aantal collega's (n=77) signaleert aandachtspunten op het terrein van faciliterende omstandigheden.

Veel van de opmerkingen (31x genoemd) gaan over de tijd die nodig is om tooling te leren gebruiken en toe te passen, een goede zoekvraag te formuleren en resultaten juist te interpreteren. Collega's benadrukken dat eerst geïnvesteerd moet worden voordat efficiency-winst optreedt.

"de grootste belemmering is de gedachte dat data-analyse leidt minder benodigde uren, maar vergeten wordt (…) dat je eerst moet investeren"

Daarnaast constateert men een aandachtpunt op het terrein van kennis (ook 31x genoemd): kennis(deling) rond (gebruik van) tooling is onvoldoende, er is te weinig bekendheid met het onderwerp en met specifieke applicaties en het ontbreekt collega's aan ervaring. Hieraan gerelateerd wordt 9x een gebrek aan scholing/opleiding/training als een belemmerende factor genoemd. 11x noemen collega's een gebrek aan (IT-)capaciteit en de beperkte mogelijkheid tot het krijgen van begeleiding of ondersteuning. Hieraan gerelateerd zien sommige collega's daarin een (grotere) rol weggelegd voor ADR Analytics.

Meer dan een kwart van de antwoorden (21x genoemd) refereert aan de beperkte beschikbaarheid van tooling (het aantal licenties en de kosten ervan) en issues rond toegang/toegankelijkheid (alleen voor bepaalde collega's/bepaalde locaties).

Inspanningsverwachting

In de reactie van 25 collega's komen punten terug die raken aan inspannings-verwachting. Het verkrijgen van data van de klant wordt door 14 respondenten als belemmerend gezien. Verschillende collega's (8x genoemd) noteren werkzaamheden die het gebruik van tooling arbeidsintensief maken: doorgronden van techniek, formuleren van de juiste vraag bij maatwerk, gebruiksklaar maken van databestanden (bijvoorbeeld om tot een bruikbaar event log te komen), juist interpreteren van uitkomsten. Dit laatste punt raakt aan het feit dat de toepassing van data-analyse aanvankelijk veel false positives oplevert: schijnbare afwijkingen die bij nadere analyse verklaarbaar zijn maar niet zomaar terzijde kunnen worden gelegd. Dit

verklaart mede waarom het gebruik van data-analyse in het begin vaak meer tijd vraagt dan een meer "traditionele" audit-aanpak.

Gewoonte
Attentiepunten die raken aan gewoonte (en houding en gedrag) worden genoemd door 24 respondenten. Specifieker wordt verwezen naar werkwijzen die traditioneel, standaard of ingesleten zijn, en het betreden van gebaande paden (9x genoemd) en terughoudend, conservatief of defensief gedrag (14x genoemd).

Complexiteit van informatiesystemen
Problemen rond informatiesystemen en de daaruit te verkrijgen data worden door 21 respondenten genoemd. Het gaat daarbij om het feit dat data verspreid zijn over meerdere systemen die soms verouderd en/of complex zijn waardoor het lastig is om er (geschikte) data aan te onttrekken (11x genoemd). Ook kan data-kwaliteit een probleem zijn door wijze van structurering of vervuiling (10x genoemd).

Sociale beïnvloeding
In de context van dit artikel vallen binnen het kader van sociale beïnvloeding onder andere de attitude jegens het gebruik van tooling van klanten, en van de leiding van de ADR. Het aantal collega's dat op dit terrein aandachtspunten signaleert is kleiner (n=11), maar de opmerkingen zijn deels scherp. Met betrekking tot de klant wordt opgemerkt dat tooling eigenlijk veel meer door de concerncontrollers opgepakt zou moeten worden, maar deze over het algemeen nog niet zover zijn.
Het toepassen van data-analyse binnen de ADR "maakt geen deel uit van de "standaardaanpak" voor audits en van medewerkers wordt niet verwacht dat zij dit toepassen". Van de leiding van de ADR verwachten verschillende collega's meer visie en daadkracht; er wordt veel gesproken over data-analyse en process mining, maar duurzame investeringen blijven volgens deze respondenten achter.

Prestatieverwachting
Met betrekking tot prestatieverwachting heeft het grootste deel van de reacties (n=9) betrekking op het toepassingsgebied van tooling: vooral geschikt voor massale gegevensverwerkende stromen, maar hiervan is lang niet bij alle onderzoeken sprake. Rechtmatigheid is moeilijk te toetsen via tooling.

3.5.2 Maatregelen die de ADR kan nemen
De tweede open vraag in de survey was: "Welke maatregelen zou de ADR kunnen nemen om de belemmeringen te verkleinen of weg te nemen?" Hierop reageerde 72% (n=131) van de respondenten.

Faciliterende omstandigheden
In lijn met de beantwoording op de eerste vraag, hebben de meeste suggesties betrekking op faciliterende omstandigheden (n=74).
Meest frequent genoemd (30x) is kennisoverdracht in allerlei varianten: opleidingen, trainingen, leergangen, kennissessies, workshops met ervaringsdeskundigen en het creëren van een omgeving waarin je iets kunt uitproberen, idealiter aan de hand van een geschikte praktijkcasus. Veel collega's vragen ook om meer tijd (17x) om tooling te kunnen toepassen en om te experimenteren. Verdere suggesties zijn het vaker delen van succesvolle praktijkvoorbeelden, meer ondersteuning en betere beschikbaarheid/een betere verdeling van tooling over de ADR.

Andere mogelijke maatregelen zijn het vergroten van kennisdeling en intensiveren van samenwerking tussen IT-ers met ervaring met tooling en de FA- en OA-collega's. Suggesties zijn het instellen van key users, het inrichten van een tool store waar collega's applicaties en uitleg kunnen vinden, en het beschikbaar maken van instructiefilmpjes en zgn. FAQs.

Sociale beïnvloeding
Maatregelen op het vlak van sociale beïnvloeding worden door 15 respondenten genoemd.
Verschillende collega's bepleiten een intensiever contact met de klant, variërend van het maken van afspraken over datalevering tot het promoten van de toegevoegde waarde van tooling en het gezamenlijk onderzoeken of data hiervoor ontsloten kan worden. Als departementen de toegevoegde waarde van tooling zien, kunnen zij verbetermaatregelen nemen om de datakwaliteit te verbeteren. Het kunnen toepassen van tooling volgens een van de respondenten een functionele eis moeten zijn voor nieuw applicaties.

Met betrekking tot de manier waarop het gebruik van tooling binnen de ADR geïntensiveerd kan worden, zijn de meningen verdeeld. Sommige collega's zijn ervoor om dit meer verplicht te stellen en het gebruik ook te verankeren in handboeken. Anderen pleiten ervoor om collega's te overtuigen via goede praktijkvoorbeelden, en oog te hebben voor tekortkomingen en weerstand.

Aan het management van de ADR vragen sommige collega's om explicieter het gebruik van tooling te ondersteunen: het spelen van een actieve(re) rol in de bijeenkomsten waar resultaten van de inzet van tooling worden gedeeld, en actief handelen en maatregelen nemen om kennis toegankelijk te maken en drempels te verlagen.

Gewoonte
Op het terrein van houding en gedrag van collega's noemen de respondenten (n=13) drie verschillende soorten maatregelen, die te categoriseren zijn als verleiding (meer training, gemixte teams), dwang (verplicht gebruik van tooling) en personeelsbeleid (gericht op instroom van IT-savvy collega's en uitstroom van collega's die niet "mee kunnen").

Complexiteit van informatiesystemen
Respondenten zijn het eens dat belemmeringen die voortkomen vanuit complexiteit van systemen of datakwaliteit alleen samen met, of door de klant zelf geadresseerd kunnen worden. Er worden verschillende niveaus genoemd met betrekking tot waar men vindt dat problemen besproken zouden moeten worden, van de zogenaamde 1e lijn (de medewerkers die direct voor een bepaald proces verantwoordelijk zijn) tot en met Rijksbrede overlegfora.

Inspanningsverwachting
Een klein aantal collega's noemt maatregelen op het terrein van inspanningsverwachting (n=5). Deze zijn vooral gericht op de moeite die het kost om data te krijgen: daarover zouden afspraken moeten worden gemaakt en vastgelegd.

4 Beschouwing en conclusie

Samenvattend heeft het onderzoek aan de hand van de onderzoeksvragen in § 1.2 tot de volgende inzichten geleid.

4.1 De betekenis van data-analyse en process mining binnen de audit

De term data-analyse heeft betrekking op een breed scala aan activiteiten om informatie te ontlenen aan data ten behoeve van de audit. Toepassingen hiervan zijn mogelijk in vrijwel alle fases van audits. Binnen data-analyse zijn verschillende groepen van technieken te onderscheiden op een spectrum dat loopt van vooral statistisch-cijfermatig naar categorisering en ordening; deze laatste vorm kan ook toegepast wor-

den op zgn. ongelabelde data zoals tekstbestanden. *Process mining* kan beschouwd worden als een specifieke vorm van data-analyse met als bijzondere eigenschap dat *dynamisch gedrag* van data zichtbaar gemaakt en onderzocht kan worden. Dit biedt de mogelijkheid om geautomatiseerde processen te onderzoeken op elementen als feitelijk procesverloop, doorlooptijden en functiescheiding.

4.2 Belemmerende factoren m.b.t. adoptie van het gebruik van IT in de audit

Een belangrijk verschil tussen de uitkomst van de workshops en de uitkomst van de survey is dat er niet zozeer een obstakel ligt op het terrein van prestatieverwachting: gemiddeld genomen (h)erkennen respondenten op de survey de voordelen die *tooling* kan bieden. Het andere aspect dat in de workshops als belangrijk naar voren kwam – **inspanningsverwachting** – is ook bij de respondenten in de survey het voornaamste punt van zorg.

In de workshops kwamen verder (in volgorde van afnemend belang) gewoonte, faciliterende omstandigheden en complexiteit van informatiesystemen naar voren als belemmerende factoren. Opvallend genoeg is de volgorde op basis van de survey *identiek*: in de volgorde op basis van gewogen gemiddelde (zie tabel 3.2) neemt **gewoonte** de 8e, **faciliterende omstandigheden** de 7e en **complexiteit van informatiesystemen** de 6e plaats in.

Het belang van deze aspecten wordt weerspiegeld in de antwoorden op de open vragen in de survey: De nadruk ligt hier duidelijk bij de faciliterende omstandigheden: 42% van alle opmerkingen gaat hierover. Vooral het gebrek aan tijd, de beperkte kennis(deling) en de beperkte beschikbaarheid van *tooling* als belemmerend gezien. Bij inspanningsverwachting wordt als struikelblok het verkrijgen van data van de klant genoemd, en de ervaring dat het (beginnen met) werken met *tooling* arbeidsintensief is. Bij gewoonte zien respondenten als belemmering dat bepaalde collega's een terughoudende attitude of traditionele werkwijze hebben. Verouderde en/of complexe systemen en vervuilde data zijn de issues bij complexiteit van informatiesystemen.

4.3 Maatregelen die interne auditdiensten kunnen treffen

Een belangrijk deel van de belemmerende factoren bevindt zich op terreinen waarop de ADR zelf maatregelen kan treffen door te zorgen voor meer tijd, meer kennisoverdracht en ondersteuning, meer *tooling* en een beleid om terughoudende medewerkers meer richting gebruik van *tooling* te bewegen:

In de survey doen de meeste collega's suggesties op het terrein van faciliterende omstandigheden: vooral maatregelen om kennisoverdracht te bevorderen en daarnaast het beschikbaar stellen van meer tijd en ondersteuning. Opvallend is dat daarnaast vooral maatregelen op terrein van gewoonte én van sociale beïnvloeding worden genoemd, onder meer over manieren om ook de meer behoudende collega's te bewegen tot het gebruik van *tooling.*

De meeste van de geopperde maatregelen liggen op het *operationele* vlak. Daarnaast zijn er maatregelen op meer *tactisch* en *strategisch* niveau denkbaar, bijvoorbeeld het adresseren van issues rond systeemcomplexiteit en datakwaliteit en het uitoefenen van *druk* richting meer uniformering in systemen binnen de hogere overlegfora van de Rijksoverheid, het voeren van strategisch personeelsbeleid en de wijze waarop leiding wordt gegeven aan de beweging richting een meer IT-*driven* controleaanpak: het kanaliseren van visie en daadkracht om veranderingen feitelijk tot stand te brengen.

5 Bibliografie

Aalst, W. (2016). *Process Mining - Data Science in Action* (second ed.). Springer.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. (2018). Analytical procedures in external auditing: A comprehensive literature survey and framework for external audit analytics. *Journal of Accounting Literature*, 83-101.

Braun, R., & Davis, H. (2003). Computer-assisted audit tools and tchniques: analysis and perspectives. *Managerial Auditing Journal, 18*(9), 725-731.

Byrnes, P., Al-Awadhi, A., Gullvist, B., & et al. (2015). Essay 3 - Evolution of Auditing: From the Traditional Approach to the Future Audit. In AICPA, *Audit analytics and continuous audit - Looking toward the future* (pp. 71-85).

Byrnes, P., Ames, B., & Vasarhelyi, M. (2015). Essay 2 - The Current State of Continuous Auditing and Continuous Monitoring. In AICPA, *Audit analytics and continuous audit - Looking toward the future* (pp. 53-70).

Financial Reporting Council. (2017). *Audit Quality Thematic Review - The Use of Data Analysis in the Audit of Financial Statements.* London: The Financial Reporting Council Ltd.

Gonsalves Jardin de Ponte, G. (2010). Risicoanalyse in de Accountantscontrole (scriptie). Universiteit van Amsterdam.

Nederlandse Beroepsorganisatie van Accountants. (2018). *NBA-bestuursvisie op beroep en beroepsorganisatie.* Amsterdam.

Pedrosa, I., & Costa, C. (2011). Models for Individual Information Technology Acceptance: a Study on Computer Assisted Audit Tools and Techniques and New Model Determinants. *IADIS Applied Computing.* Rio de Janeiro. doi:10.13140/RG.2.1.2968.0804

Protiviti. (2018). Analytics in Auditing is a Game Changer - Internal Audit Capabilities and Needs Survey.

Roos Lindgreen, E. (2016). From IT Auditor to Data Scientist. *EDPACS, 53*(3), 1-4.

Rosli, K., Yeow, P., & Siew, E. (2012). Factors Influencing Audit Technology Acceptance by Audit Firms: A New I-TOE Adoption Framework. *Journal of Accounting and Auditing: Research & Practice*, 1-11.

Stewart, T. (2015). Essay 5 - Data Analytics for Financial Statement Audits. In AICPA, *Audit analytics and continuous audit - Looking toward the future* (pp. 105-128).

Venkatesh, V., Morris, G., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27 (3)*, 245-278.

Venkatesh, V., Thong, J., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly, 36*(1), 157-178.

Software Asset Management en het in control zijn van organisaties

Leon Huijsman

Met een juridisch diploma op zak startte Leon in 2010 bij WireITup, een IT-bedrijf in het MKB. Na twee jaar maakte hij de overstap naar KPMG Advisory, om deel uit te maken van het Contract Compliance Services team. Met een focus op zowel IT-audits als software license compliance was de stap naar het volgen van de uitdagende Executive Master IT Audit, Compliance & Advisory snel gemaakt.
Na zes jaar KPMG werd Leon in juni 2018 ingelijfd door CRH om daar als Software Asset Manager aan de slag te gaan. Bij CRH, een wereldwijde speler in bouwmaterialen, richt Leon zich op het opzetten van een Europees Software License Compliance programma.

1 Software Asset Management uiteengezet

Om een zo volledig mogelijk beeld te krijgen van wat SAM precies inhoudt wordt in de eerste paragraaf van dit hoofdstuk ingegaan op de definitie van SAM. Wat houdt het precies in, welke karakteristieken kenmerken SAM en wat valt binnen of buiten de scope van SAM? Hiernaast worden mogelijke doelstellingen voor organisaties behandeld welke gerealiseerd kunnen worden met SAM.

1.1 Wat is Software Asset Management?

Zoals in de inleiding al werd aangehaald heeft het SAM proces tot nu toe weinig wetenschappelijke aandacht gekregen. Hoewel in de IT management wereld SAM een relatief bekend begrip aan het worden is, ontbeert het nog steeds een academisch erkende definitie. Het is dan ook een uitdaging om SAM duidelijk in kaart te brengen.

ITIL omschrijft SAM als alle infrastructuur en processen welke noodzakelijk zijn voor het effectief managen, controleren en beschermen van software bezittingen binnen een organisatie, door alle fasen van de software levenscyclus. Het managen van hardware bezittingen valt buiten deze definitie voor zover deze niet noodzakelijk zijn voor een efficiënt SAM proces. Deze definiëring komt min of meer overeen met de definitie welke is neergelegd in ISO/IEC 19770-1: het effectieve management, de controle en bescherming van software middelen binnen in een organisatie, en het effectieve management, controle en bescherming van informatie ten aanzien van gerelateerde middelen welke benodigd zijn om software middelen te managen. Kortgezegd omvat SAM het totale proces rondom het beheer en de optimalisatie van de planning, inkoop, implementatie, onderhoud en uitfasering van softwarepakketten binnen organisaties. Deze activiteiten dienen uiteindelijk te leiden tot een adequaat administratief beheer ten aanzien van de IT middelen van een organisatie.

In hoofdstuk 3 wordt nader ingegaan op de ITIL en ISO/IEC 19770-1, uit welke processen deze zijn opgebouwd, wat de exacte scope hiervan is en op welke wijze deze toegepast kunnen worden binnen organisaties.

Uit voorgaande begripsbepalingen van ITIL en ISO/IEC 19770-1 kunnen een aantal karakteristieken worden ontleend.

- SAM is een zakelijke praktijk waarbij zowel technologie, processen als mensen betrokken zijn;
- SAM heeft voornamelijk betrekking op software welke de meeste impact heeft op de bedrijfsvoering van een organisatie. Dit houdt concreet in dat gezien de operationele impact SAM zich meer richt op serversoftware dan op software op werkstations;
- Vaak zijn binnen organisaties meerdere afdelingen betrokken bij SAM, denk hier bijvoorbeeld aan IT, Legal, Finance, HR en Procurement. SAM is dan ook een multidisciplinair proces;
- SAM betreft niet alleen een implementatietraject, maar tevens het continu onderhouden hiervan.

In de volgende paragraaf wordt ingegaan op het feit waarom SAM van belang is voor organisaties en wat de mogelijk te behalen voordelen zijn.

1.2 Waarom SAM?

Wet- en regelgeving

Zoals in de inleiding van dit hoofdstuk al werd aangehaald is het voor organisaties van belang om in het kader van corporate governance inzicht te hebben in de aanwezige software middelen binnen een organisatie. Deze middelen zijn veelal van primair belang om de continuïteit van de organisatie te kunnen waarborgen en hebben daarnaast betrekking op juridische- en contractuele verplichtingen. Organisaties worden vanuit wet- en regelgeving steeds meer gedwongen om deze belangrijke middelen inzichtelijk te maken in het kader van de betrouwbaarheid van hun financiële verslaglegging. Denk hierbij bijvoorbeeld aan de Sarbanes-Oxley wetgeving (afgekort SOx) in de Verenigde Staten, welke werd ingevoerd als reactie op een

aantal grote financiële schandalen (onder andere Arthur Andersen, Enron en WorldCom). Een van de primaire doelstellingen van SOx betreft interne controle en hierbij wordt specifiek de nadruk op controle ten aanzien van IT gelegd. In control zijn met betrekking tot IT is volgens SOx van cruciaal belang om interne controle te bewerkstelligen. In de Nederlandse wetgeving ligt de wettelijke verplichting om in control te zijn ten aanzien van software middelen impliciet verankerd in de accountantsverklaring van artikel 2:393 van het Burgerlijk Wetboek. In het vierde lid van dit artikel wordt ingegaan op IT:

> *(…)Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.*

De controlerend accountant van een organisatie moet dus een uitspraak doen over de betrouwbaarheid en continuïteit van de IT omgeving. Om een dergelijke uitspraak te kunnen doen is allereerst van belang dat er overzicht is ten aanzien van de hoeveelheid gebruikte software middelen binnen een organisatie. Programmatuur die onbekend is en niet gemanaged wordt binnen een organisatie kan een potentieel beveiligingsrisico vormen en derhalve van impact zijn op de continuïteit van de IT omgeving (en dus geautomatiseerde gegevensverwerking). De software wordt dan immers niet voorzien van de nieuwste updates en patches waardoor deze een risico voor de organisatie vormt.

Naast het feit dat SAM van belang is om te voldoen aan toepasselijke regelgeving worden in de literatuur ook mogelijke voordelen ten aanzien van de bedrijfsvoering van organisaties herkend.

Potentiële voordelen en doelstellingen van SAM

In ISO/IEC 19770-1 en ITIL worden een aantal doelstellingen van SAM herkend en onder een drietal categorieën ondergebracht, te weten: risicomanagement, controle ten aanzien van kosten en voordeel ten opzichte van concurrentie door het realiseren van efficiëntie voordelen.

Met betrekking tot risicomanagement kan SAM een mitigerende werking hebben ten aanzien van een aantal algemeen erkende bedrijfsrisico's. Een hiervan is het juridische- en financiële risico als gevolg van het niet voldoen aan licentievoorwaarden ten aanzien van gebruikte programmatuur. Hoewel theoretisch gezien algemene opsporingsdiensten en bijvoorbeeld de BSA bij een organisatie kunnen zorgen voor blootstelling aan dit risico vormen de leveranciers van de software zelf het grootste risico. Licentieovereenkomsten gaan vaak vergezeld van een audit clausule waardoor softwareleveranciers zich het recht voorbehouden om periodiek een audit bij de afnemer van de software te initiëren. Reden om een organisatie te auditen kan verschillende oorzaken hebben, zoals een bepaald aankoopgedrag van licenties of opzegging van alle overeenkomsten in combinatie met een voorgenomen overstap naar een andere softwareleverancier. Risico's kunnen zich openbaren als gevolg van geïnstalleerde software waar geen licenties voor zijn afgenomen, verlies (kwijtraken) van licenties welke zijn aangekocht, complexe licentieregels welke onbewust worden overtreden en ten slotte het afgaan op onjuiste informatie vanuit resellers van software.

Een dergelijke audit kan binnen een organisatie een aanzienlijk financieel risico met zich meebrengen. Niet alleen in de aanschaf van nieuwe licenties (die de organisatie misschien niet eens nodig heeft), maar tevens het beschikbaar stellen van resources om het gebruik van de software weer in overeenstemming met de licentieregels te brengen. Verder bestaat er een kans op reputatieschade, al lijken de softwareleveranciers en licentieafnemers weinig baat te hebben om resultaten van audits openbaar te maken.

Een ander voordeel wat met SAM gerealiseerd kan worden is het minimaliseren van beveiligingsrisico's als gevolg van het inadequaat managen van security patches en andere software updates. De aanwezigheid van verouderde software levert potentieel beveiligingsrisico's op aangezien deze niet is uitgerust met het meest actuele beveiligingsniveau. Het bijhouden van software updates vermindert dan ook de kans op continuïteitsproblemen binnen organisaties. Veelal vinden updates van applicaties niet op geautomatiseerde wijze plaats waardoor hiervoor een procedure aanwezig dient te zijn om deze toch periodiek en tijdig uit te kunnen voeren. Het minimaliseren van beveiligingsrisico's zorgt er weer voor dat kansen op interrupties van de berdrijfsvoering worden verminderd.

Uit bovenstaande blijkt dat de risico's die met behulp van SAM kunnen worden gemanaged zeer divers zijn. De tweede categorie van doelstellingen betreft kostenbesparingen die organisaties kunnen realiseren. Wanneer een organisatie een accuraat beeld heeft van welke licenties er daadwerkelijk beschikbaar zijn,

welke er daadwerkelijk gebruikt worden (ofwel de licentiepositie van de organisatie) en welke er ten slotte wenselijk zijn, verbetert de onderhandelingspositie aanzienlijk. Er zullen immers geen licenties worden aangeschaft waar de organisatie al recht op heeft of licenties die het bedrijf eigenlijk niet nodig heeft. Kennis van geïnstalleerde software binnen een organisatie brengt ook efficiënter gebruik van de ondersteunende hardware met zich mee. Verder zal een juist ingericht SAM de operationele kosten van een organisatie uiteindelijk verminderen.
Ten slotte kan SAM aanzienlijke efficiencyvoordelen met zich meebrengen. Een duidelijk beeld van de beschikbare software middelen biedt mogelijkheden om deze kwalitatief beter te managen. De transparantie in het management van de IT omgeving zal toenemen. Wanneer er bijvoorbeeld verschillende afdelingen zijn kunnen deze aan de hand van dezelfde criteria worden behandeld. Verder kan SAM zorgen voor de mogelijkheid om snel nieuwe functionaliteiten binnen organisaties uit te rollen waardoor deze snel in gebruik kunnen worden genomen. Daarnaast kan een transparant SAM proces ervoor zorgen dat overnames en fusies tussen partijen soepeler verlopen.
Concluderend kan worden gesteld dat de voordelen die met SAM behaald kunnen worden drieledig zijn; het realiseren van kostenbesparingen, controle ten aanzien van risico's en het behalen van meer efficiëntie. Hoofdstuk 3: Frameworks en bestaande methodologieën ten aanzien van SAM

2 Frameworks en bestaande methodologieën ten aanzien van SAM

Ten aanzien van SAM zijn diverse standaarden beschikbaar die als handvat kunnen dienen bij implementatie van SAM bij organisaties. In deze paragraaf worden de bekendste standaarden kort uiteengezet. In het volgende hoofdstuk zullen de kritische succesfactoren voor een succesvolle SAM organisatie uit deze standaarden worden geïdentificeerd.

2.1 Samenvatting, raakvlakken en conclusie

In voorgaande paragrafen zijn respectievelijk CobiT, ISO 19770/IEC-1 en ITIL behandeld. De nadruk lag hierbij op de koppeling van de frameworks aan de algemene SAM doelstellingen: het realiseren van kostenbesparingen, het bereiken van efficiencyvoordelen en het managen van risico's.

2.1.1 Samenvatting frameworks en methodologieën

CobiT

CobiT is een raamwerk gericht op het gestructureerd inrichten en beoordelen van een IT-beheeromgeving. Het is een best practice die organisaties in staat stelt om adequate beheersmaatregelen te stellen. CobiT is primair op de business georiënteerd en kan als leidraad dienen voor het management en voor proceseigenaren van een organisatie. Omdat CobiT een breed spectrum heeft, is gekeken waar de diverse CobiT domeinen op SAM toegepast kunnen worden. Per CobiT domein is naar de aanwezige processen gekeken en bepaald of hier een al dan niet grote overlap met SAM bestaat. Uit Hoofdstuk 3.1 is gebleken dat alle domeinen (*Plan and Organise, Acquire and Implement, Deliver and Support* en *Monitor and Evaluate*) meerdere processen bevatten die in meer of mindere mate op SAM toegepast kunnen worden.
Binnen het *Plan and Organise* domein worden onder andere eisen ten aanzien van de IT-architectuur van een organisatie gedefinieerd hetgeen een solide basis dient te vormen om IT te managen met zo min mogelijk operationele problemen. De basis voor de controle omgeving van SAM wordt in dit domein gelegd. Requirements ten aanzien van personeel, capaciteiten en verantwoordelijkheden worden bepaald en budgeten beschikbaar gesteld. Tevens kan een kwaliteitsmanagementsysteem worden ingevoerd om ontwikkeling en aanschaf van IT gerelateerde middelen zoals software te kunnen bewerkstelligen. Ten slotte kan binnen het *Plan and Organise* domein met *PO9 Assess and manage IT risks* een framework worden ontwikkeld ten aanzien van risicomanagement.

Het *Acquire and Implement* richt zich op processen met betrekking tot de aanschaf en het onderhoud van software en andere IT middelen. Licenties, licentievoorwaarden en de software dienen zorgvuldig bewaard te worden en beschikbaar te zijn. Door middel van periodieke inventarisaties kan worden vastgesteld of procedures ten aanzien van softwarebeheer nog actueel zijn. Ook het change management valt binnen dit domein en is van toepassing op SAM. Periodiek dienen nieuwe versies en patches geïnstalleerd te worden volgens dit proces, om ervoor te zorgen dat er een impactanalyse op voorgestelde changes plaatsvindt en deze uiteindelijk op gestructureerde wijze wordt uitgevoerd.
Binnen het *Delivery and Support* domein is in het bijzonder *DS9 Manage the Configuration* op SAM van toepassing, hiermee kan de SAM database worden gemaakt en onderhouden. Het is immers van vitaal belang voor een organisatie dat duidelijkheid bestaat omtrent de aanwezige licenties en geïnstalleerd/toegewezen software. Ten slotte wordt binnen het *Monitor and Evaluate* domein zorggedragen voor optimalisatie van bestaande processen. Tevens ligt de focus op compliance met externe regelgeving, waaronder in het geval van SAM toepasselijke licentievoorwaarden.

ISO
Met ISO/IEC 19770-1 is een erkende standaard voor SAM opgenomen die zich richt op implementatie van SAM binnen een organisatie aan de hand van een viertal Tiers. Met een conceptueel raamwerk kunnen de doelstellingen van de verschillende Tiers worden bereikt. Dit zijn respectievelijk: *Organizational Management Processes for SAM, Core SAM Processes* en *Primary Process interfaces for SAM*, welke weer kunnen worden onderverdeeld in subcategorieën.
De eerste Tier richt zich op het bewerkstelligen van betrouwbare data. Dit is immers een voorwaarde om de doelstellingen van SAM te kunnen bereiken. Voornamelijk de volledigheid en juistheid van data vormen hierbij belangrijke uitgangspunten. Dit vormt de basis voor de hoogst erkende prioriteit van SAM, licentie compliance. *Tier 1* richt zich primair op het inrichten van processen om software assets te kunnen identificeren aan de hand waarvan een licentiepositie kan worden gecreëerd.

Tier 2 van ISO richt zich op het praktische management zoals het verbeteren van management controle en voordelen hieruit. Risico's zijn geïdentificeerd en verantwoordelijkheden hieromtrent toegewezen. Denk hierbij aan het verzekeren dat verantwoordelijkheden ten aanzien van software gebruik worden erkend door het bestuur van de organisatie. Verder wordt *Tier 2* zich onder andere op het zorgdragen dat de organisatie beschikt over de juiste SAM expertise en het onderhouden hiervan. De doelstellingen van *Tier 2* zijn dan ook tweeledig, het behalen van quick wins en het creëren van een controleomgeving.

In *Tier 3* wordt SAM geïntegreerd met andere operationele processen binnen de organisatie waardoor meer effectiviteit en efficiëntie wordt bereikt. De van toepassing zijnde processen richten zich grotendeels op de integratie met overige operationele processen die in overeenstemming zijn met andere ISO normen, zoals ISO/IEC 12207, System and Software Engineering en ISO/IEC 20000, IT Service Management. De nadruk wordt gelegd op de belangrijkste software lifecycle processen zoals acquisitie, gebruik en uitfasering en integratie hiervan met andere operationele bedrijfsprocessen.
De laatste Tier van ISO is bereikt wanneer SAM niet alleen is geïntegreerd in de operationele processen, maar tevens is opgenomen in de strategische planning van de organisatie. SAM voldoet verder aan alle in ISO/IEC 19770-1 gestelde eisen. Zo vindt continu toezicht plaats of de doelstellingen van SAM zijn bereikt en waar er nog verbetering mogelijk is. Tevens voldoen alle SAM processen aan toepasselijke eisen ten aanzien van informatiebeveiliging (zoals neergelegd in ISO/IEC 27001).

ITIL
ITIL richt zich op IT Service Management binnen een organisatie. ITIL benadrukt dat de overkoepelende doelstelling van SAM ligt in een goed werkende corporate governance structuur. Aan de hand van een

schaalbare en gestructureerde benadering kan dit worden bewerkstelligd. Het ontwikkelen van een duidelijke visie en strategie van het management van een organisatie wordt in ITIL aangemerkt als eerste belangrijke fase. Deze dienen in lijn te liggen met de algemene doelstellingen van de organisatie. Belangrijk hierbij is dat de risico's die aan softwaregebruik verbonden zijn bekend zijn bij de organisatie.
Daarna dient een algemeen beleid ten aanzien van SAM te worden opgesteld en gecommuniceerd binnen de organisatie. Het beleid moet periodiek kunnen worden herzien indien dit wenselijk wordt geacht naar aanleiding van bijvoorbeeld een uitgevoerde risico assessment. Verder zorgt het management dat personen met verantwoordelijkheden ten aanzien van SAM voldoende capaciteiten hebben om deze uit te kunnen voeren. Verder richt ITIL zich op het ontwikkelen en implementeren van SAM processen en procedures. Het doel van de *'Overall management processes'* is het bewerkstelligen en onderhouden van een management infrastructuur waarbinnen SAM processen kunnen worden geïmplementeerd. Hieronder vallen logistieke processen, relationele (met onder andere softwareleveranciers) en asset management processen, die erop gericht zijn om software te herkennen en onderhouden. Essentieel is hierbij de *SAM Database*, die de basis vormt voor een goed functionerend SAM systeem door te beschikken over volledige en juiste informatie. Nadat SAM is geïmplementeerd zal er doorlopend onderhoud plaatsvinden aan de SAM database om de informatie die hierin is opgeslagen in overeenstemming te houden met aanverwante disciplines zoals *continuity of operations* en *capacity management*. Regelmatige review en verbetering dient plaats te vinden om efficiency en effectiviteit van SAM processen te vergroten.

2.1.2 Conclusie

In dit hoofdstuk zijn drie verschillende methodologieën nader bekeken. Allereerst is gekeken naar CobiT en welke raakvlakken er zijn tussen SAM en de CobiT domeinen en processen. Uit deze uiteenzetting is gebleken dat er op meerdere facetten raakvlakken zijn met SAM, maar dat deze weinig concreet zijn omdat CobiT zich richt op IT-beheersing in algemene zin. CobiT helpt SAM dus wel met de plaatsing in een breder controleperspectief, maar biedt weinig concrete handvatten om SAM tot een succes te maken. In het volgende hoofdstuk zal nader worden bekeken of en zo ja welke aspecten meegenomen kunnen worden in het op te stellen framework.
Ten aanzien van ISO kan worden gesteld dat er voldoende concrete eisen worden gesteld om SAM succesvol te kunnen implementeren. In de norm wordt echter niet ingegaan op de wijze waarop deze eisen gerealiseerd dienen te worden waardoor het onwaarschijnlijk is dat SAM succesvol geïmplementeerd kan worden op basis van alleen ISO. Een combinatie met een andere best practice ligt dan ook meer voor de hand. Door het hanteren van verschillende Tiers wordt tegemoet gekomen aan verschillende ambitieniveaus van organisaties. Nadeel hiervan is dat pas bij het bereiken van de laatste Tier alle mogelijke doelstellingen van SAM bereikt kunnen worden. Gezien de hoeveelheid normen kan vraagtekens gesteld worden bij de haalbaarheid hiervan in de praktijk en of de te bereiken voordelen dan opwegen tegen de gemaakte kosten en inspanningen van de organisatie. Verder ontbreekt het aan duidelijk meetindicatoren op basis waarvan vastgesteld kan worden dat een bepaald stadium is bereikt.
Het derde behandelde framework, ITIL, richt zich meer op het operationeel management niveau en de wijze waarop SAM geïmplementeerd kan worden binnen een organisatie. ITIL biedt dan ook concretere handvatten dan ISO ten aanzien van de implementatie. ITIL maakt aan de hand van een aantal principes gebruik van een schaalbare en gestructureerde benadering. Voor integratie van SAM met overige bedrijfsprocessen wordt echter verwezen naar andere ITIL modules, waardoor een SAM implementatie meer zal omvatten als de normen genoemd in deze specifieke ITIL best practice.
Na analyse blijkt dat de behandelde methodologieën allen handvatten bieden ten aanzien van SAM, maar dat het hanteren van één enkele methodologie waarschijnlijk onvoldoende is om SAM op succesvolle wijze te implementeren. Het ligt dan ook voor de hand om voor het theoretisch kader een combinatie te gebruiken. In het volgende hoofdstuk zal op basis van de behandelde methodologieën een framework worden opgesteld aangevuld met eigen ervaringen.

3 Best practice en kritische succesfactoren van SAM

In het vorige hoofdstuk zijn achtereenvolgens CobiT, ISO en ITIL behandeld. Deze frameworks bieden allen handvatten om SAM te implementeren bij een organisatie. Op een aantal vlakken op het gebied van SAM vertonen de frameworks een grote overlap met elkaar, ook deze zijn in het vorige hoofdstuk behandeld. In dit hoofdstuk zal aan de hand van de behandelde methodologieën en eigen ervaringen een best practice worden opgesteld om aan de hand hiervan de belangrijkste kritische succesfactoren te identificeren.

Best Practice

Uit bovenstaande uiteenzetting is gebleken dat CobiT niet als leidraad voor de best practice zal worden gebruikt, omdat deze vanwege de brede scope niet gedetailleerd genoeg is om SAM te kunnen implementeren. Uiteraard kunnen er wel bepaalde aspecten van CobiT gebruikt worden. Ten aanzien van ISO kan worden gesteld dat deze concrete normen bevat waar een organisatie aan dient te voldoen om de doelstellingen van SAM te bereiken. Wel zijn vraagtekens geplaatst bij het praktische nut van Tier 4. ITIL richt zich primair op de 'hoe' vraag, welke van belang is bij implementatievraagstukken. Een combinatie van de frameworks ligt dan ook voor de hand bij het opstellen van de best practice.

Category	Sub Category	KSF
Organizational Management Processes	SAM Planning, Implementation and Improvement	SAM Capabilities SAM Resources Management Awareness Management Hierarchy Management Sponsorship
	Corporate Governance for SAM	
SAM Inventory Processes	Software Asset Identification and Accuracy of Inventory	SAM Capabilities SAM Database SAM Resources
	Software Asset Inventory Management (both hard- and software)	
Software License Compliance	License Entitlement Inventory	SAM Technical Capabilities SAM Entitlement Capabilities SAM Database
	Conformance Verification	
Operations Management Processes and Interfaces	Operations Management Interfaces	Budget SAM Resources
Life Cycle Process Interfaces	Planning Process	SAM Capabilities SAM Database
	Acquisition Process	
	Software Deployment process	
	Retirement Process	

In bovenstaand framework is voor wat betreft de gekozen categorieën aansluiting gezocht bij ISO. Bij het opstellen van de subcategorieën is zowel gekeken naar ISO, ITIL maar ook CobiT (ten aanzien van corporate governance) en de eigen ervaringen. Vanuit mijn werkzaamheden als software licentie auditor en adviserende rol ten aanzien van SAM vraagstukken heb ik namelijk zicht op veel praktische en concrete problemen waar organisaties tegenaan lopen tijdens implementatie van SAM. Bovendien heb ik vanuit mijn rol als auditor zicht op de aspecten waar door softwareleveranciers belang aan wordt gehecht. In de volgende paragraaf wordt toegelicht waarom voor deze (sub)categorieën en KSFen gekozen is.

Toelichting best practice

Ten aanzien van de subcategorieën is gekeken naar de categorieën welke voor ISO voornamelijk in Tier 1,2 en 3 van belang zijn. Er zijn nog geen organisaties bekend die ISO 19770-1 voor Tier 4 zijn gecertificeerd dus is hier in het kader van de haalbaarheid van de best practice minder aandacht aan besteed.

Organizational Management Processes

Bestaande uit de subcategorieën *SAM Planning, Implementation and Improvement* en *Corporate Governance for SAM* vormt dit de basis voor een succesvolle SAM. Ten aanzien van SAM dienen er gedocumenteerde procedures en processen opgesteld te worden, rollen en verantwoordelijkheden worden toegekend aan de juiste personen en het ambitieniveau ten aanzien van SAM te worden bepaald. Op basis van het ambitieniveau en de beschikbare capaciteit met voldoende SAM capabilities kan een planning voor de implementatie van SAM worden opgesteld. Het toekennen van voldoende personeel met toereikende kwaliteiten is verder een voorwaarde om SAM succesvol te implementeren (KSF *SAM Resources* en *Capabilities*). Een absolute voorwaarde voor een succesvolle SAM is de ondersteuning en bewustzijn vanuit het management. Allereerst dient het management van een organisatie zich bewust te zijn van de noodzaak van SAM en het ambitieniveau hieromtrent te bepalen. Vanuit onze eigen ervaringen zien wij dat organisaties het belang van SAM vaak pas in gaan zien nadat een licentie audit heeft plaatsgevonden met negatieve financiële consequenties. Pas dan wordt SAM op de agenda van het management gezet en wordt er budget, capaciteit en prioriteit aan toegekend. Daarom is in het framework de KSF *Management Awareness* opgenomen. Verder is de KSF *Management Support* opgenomen, deze dient namelijk doorlopend ondersteuning te bieden. In mijn ogen ligt er in het bijzonder een hiërarchische rol voor het management. SAM processen raken binnen een organisatie namelijk veel verschillende afdelingen die qua hiërarchie gelijkwaardig aan elkaar zijn. Het is niet ondenkbaar dat er tijdens een SAM traject conflicterende beslissingen genomen moeten worden. Van grote waarde is in dat geval de aanwezigheid van het management dat met kennis van zaken bepaalde beslissingen kracht kan bijzetten. KSF *Management Hierarchy* is daarom in het framework opgenomen.

SAM Inventory Processes

De inventory processen zijn verder van groot belang voor SAM. Tier 1 van ISO heeft het hebben van betrouwbare data als uitgangspunt en de genoemde subcategorieën in het bovenstaande framework richten zich op het verkrijgen van betrouwbare data. Het hebben van een SAM Database die juist en volledig is, kan dan ook als voorwaarde en KSF worden onderkend. Om dit te bewerkstelligen is voldoende personeel met de juiste capaciteiten een absolute voorwaarde. Technische kennis ten aanzien van software is vereist om deze database goed te kunnen vullen. Software dient immers op juiste wijze geïdentificeerd te kunnen worden.

Software License Compliance

Ten aanzien van categorie Software License Compliance wordt hier afgeweken van ISO en meer aansluiting gezocht bij ITIL. Dezelfde voorwaarden als bij de *SAM Inventory Processes* zijn van toepassing. In mijn ogen is dit het belangrijkste aspect van SAM en wordt hier in de bestaande frameworks onvoldoende aandacht aan besteed. Deze fase richt zich immers op compliant zijn. Dit is enerzijds gelegen in de licentiepositie van de klant, maar anderzijds dient gekeken te worden of het gebruik van de software in overeenstemming met de geldende gebruikersvoorwaarden is. Voornamelijk aan dit laatste aspect wordt in zowel CobiT, ISO als ITIL te weinig aandacht besteed. Er wordt voorbijgegaan aan de complexiteit en onduidelijkheid van de licentieregels enerzijds en aan de andere kant de praktijk waar in een organisatie van (voornamelijk) technisch beheerders van de software wordt verlangd dat deze optimaal functioneert. Mijn ervaring is dat deze twee werelden (de 'juridische' gebruikersvoorwaarden kant ten opzichte van de beheerders) vaak niet voldoende communiceren en dat beide partijen elkaars belangen onvoldoende onderkennen. Het is dus van groot belang dat er, naast een SAM Database met juiste en volledige informatie, voldoende personeel aanwezig is met kennis van SAM ten aanzien van zowel licentieregels als functioneel beheer van de applicatie. Daarom is ten aanzien van de KSF *SAM Capabilities* bij *Software License Compliance* onderscheid gemaakt tussen technische kennis ten aanzien van software en kennis ten aanzien van de voorwaarden aan het gebruik. Wanneer deze capaciteit binnen een grote organisatie niet aanwezig is hangt compliant zijn meer van geluk dan van wijsheid af.

Operations Management Processes and Interfaces
Zaken zoals operationeel management binnen de organisatie ten aanzien van SAM (Contract Management, Financieel Management en Service Level Management) dienen aanwezig te zijn. Hierbij vormen voldoende budget en personeel een voorwaarde om dit succesvol ten uitvoer te brengen. Deze categorie richt zich in mijn ogen voornamelijk op de realisatie van kostenbesparingen door middel van bijvoorbeeld het efficiënter kunnen inkopen van software en het hiermee kunnen bereiken van efficiencyvoordelen.

Life Cycle Process Interfaces
Ten slotte is optimalisatie van de gehele software lifecycle een belangrijke voorwaarde om de doelstellingen van SAM te bereiken. Specifieke aandacht is hier weggelegd op het plannings-, acquisitie-, gebruiks- en uitfaseringsproces. Uitgangspunt is hier dat de organisatie beschikt over een juiste en volledige SAM database zodat beslissingen genomen kunnen worden op basis van kwalitatief goede informatie. Hiernaast zijn SAM capabilities een voorwaarde. In de planningsfase is het bijvoorbeeld van belang dat er een proces aanwezig is aan de hand waarvan geïdentificeerd kan worden wat de behoefte binnen de organisatie is ten aanzien van bepaalde software en binnen welke termijn deze operationeel dient te zijn. Ten aanzien van het acquisitieproces gelden dezelfde eisen. Personeel belast met bijvoorbeeld contractonderhandelingen zal voldoende kennis moeten hebben ten aanzien van de verschillende opties met betrekking tot licenties. Uiteraard zijn deze capaciteiten ook van belang tijdens het deployment- en uitfaseringsproces. Er dient een proces aanwezig te zijn zodat licenties van vertrekkend personeel ingetrokken worden en indien mogelijk hergebruikt. De KSF *SAM Database* is dan ook van belang ten aanzien van de gehele software lifecycle.
In het volgende hoofdstuk zal aan de hand van een tweetal interviews met experts ten aanzien van SAM worden getoetst of het voorgestelde framework volledig en juist is. Tevens zal worden ingegaan op de praktische haalbaarheid van het framework.

4 Case Study

In Hoofdstuk 4 is op basis van beschreven methodologieën, best practices en eigen ervaringen een framework opgesteld. Dit framework bevat een aantal kritische succesfactoren welke aanwezig dienen te zijn om de doelstellingen van SAM binnen een organisatie te kunnen realiseren. In dit hoofdstuk wordt dit theoretische framework getoetst aan de praktijk. Door middel van een tweetal interviews met experts op het gebied van SAM wordt het framework getoetst op praktische haalbaarheid. Daarnaast worden de opgestelde kritische succesfactoren beoordeeld op juistheid en volledigheid. Tevens wordt geïnventariseerd of het framework als zodanig volledig is of dat er wellicht bepaalde aspecten weggelaten kunnen worden.
Na analyse van de onderzoeksresultaten wordt in Hoofdstuk 6 bepaald of de bevindingen leiden tot aanpassing van het framework.

4.1 Samenvatting case study
Concluderend kan worden gesteld dat uit de case study aanvullingen zijn gekomen die input kunnen vormen om het framework verder vorm te geven. Ondanks dat de geïnterviewden bij verschillende typen organisaties werkzaam zijn worden zij geconfronteerd met vergelijkbare uitdagingen.
Per categorie van het framework is gekeken of deze volledig en juist is en of deze praktisch haalbaar is. De toevoegingen die geïnterviewden hadden richtten zich met name op het cultuuraspect van de organisatie en het support/mandaat vanuit het management (en het zorgdragen door middel van rapportages dat deze support gehandhaafd blijft). Verder zijn de geïnterviewden van mening dat naast cultuur en management support, awareness bij het management en betrokken partijen een cruciale voorwaarde is om SAM succesvol te kunnen implementeren.

Indien voorzien van deze aspecten kan het framework als hulpmiddel dienen om de doelstellingen van SAM te realiseren. In het volgende hoofdstuk zal het theoretisch framework worden aangepast en aangevuld met toevoegingen uit de case study.

5 Analyse en Bevindingen

In het vorige hoofdstuk is het theoretisch framework door middel van een case study aan de praktijk getoetst. Aan de hand van een tweetal interviews is het framework getoetst op juistheid, volledigheid en praktische haalbaarheid. In dit hoofdstuk worden de bevindingen uit de interviews nader geanalyseerd en zal worden bepaald of deze leiden tot nuancering van het framework.
Uit de gesprekken is gebleken dat de gekozen categorisering van het framework logisch voorkomt en geen aanpassing behoeft. De gekozen categorieën en subcategorieën dekken alle SAM aspecten binnen een organisatie af. De indeling is op de ISO standaard gebaseerd en wijkt alleen af ten aanzien van de categorie *Software License Compliance*, die is opgenomen omdat er in de beschreven standaarden te weinig nadruk wordt gelegd op de complexiteit van licentievoorwaarden en het belang van naleving hiervan.

5.1 Nuancering framework

Voorgaande uiteenzetting heeft geleid tot een nadere specificering van het theoretische framework. Er zijn zoals hierboven besproken diverse KSFen toegevoegd en nader uitgewerkt.

Category	Sub Category	KSF
Organizational Management Processes	SAM Planning, Implementation and Improvement	1. **Budget** -> voldoende budget om doelstellingen te kunnen realiseren 2. **SAM Capabilities** -> personeel beschikt over juiste kennis ten aanzien van SAM 3. **SAM Resources** -> voldoende FTE om doelstellingen te kunnen realiseren 4. **Awareness Management/Personeel** -> op structurele wijze zorgen voor bewustheid management/overige betrokkenen ten aanzien van SAM 5. **Management Hierarchy** -> Indien noodzakelijk kunnen beslissingen worden afgedwongen 6. **Management Sponsorship** -> door neerleggen juiste mandaten in organisatie en structurele ondersteuning van verantwoordelijken 7. **Rapportage** -> stakeholders op de hoogte houden om bewustzijn te vergroten en support te behouden
	Corporate Governance for SAM	
SAM Inventory Processes	Software Asset Identification and Accuracy of Inventory	1. **SAM Capabilities** -> personeel beschikt over juiste kennis ten aanzien van SAM 2. **SAM Databases** -> registraties van gebruik, aanwezige assets en beschikbare licenties. Focus op juistheid informatie en volledige dekking binnen organisatie. 3. **SAM Resources** -> voldoende FTE om doelstellingen te kunnen realiseren 4. **Rapportage** -> stakeholders op de hoogte houden om bewustzijn te vergroten en support te behouden
	Software Asset Inventory Management (both hard- and software)	
Software License Compliance	License Entitlement Inventory	1. **SAM Technical Capabilities ->** Functioneel beheerders met bewustzijn en kennis ten aanzien van configuraties/ mogelijke implicaties licentievormen 2. **SAM Entitlement Capabilities ->** Kennis van gebruiksvoorwaarden en mogelijke optimale licentievormen 3. **SAM Databases** -> registraties van gebruik, aanwezige assets en beschikbare licenties. Focus op juistheid informatie en volledige dekking binnen organisatie. 4. **Closed loop** -> alle assets zijn continu traceerbaar
	Conformance Verification	
Operations Management Processes and Interfaces	Operations Management Interfaces & Service Level Management	1. **Budget** -> voldoende budget om doelstellingen te kunnen realiseren 2. **SAM Resources** -> voldoende FTE om doelstellingen te kunnen realiseren
Life Cycle Process Interfaces (both hard- and software)	Planning Process	1. **SAM Capabilities** -> personeel beschikt over juiste kennis ten aanzien van SAM 2. **SAM Databases** -> registraties van gebruik, aanwezige assets en beschikbare licenties. Focus op juistheid informatie en volledige dekking binnen organisatie 3. **Closed loop** -> alle assets zijn continu traceerbaar
	Acquisition Process	
	Software Deployment Process	
	Retirement Process	

5.2 Conclusie

Vanuit de case study zijn diverse nuanceringen op het framework aangebracht. Deze nuanceringen hebben voornamelijk betrekking gehad op het realiseren van continue support vanuit het management en alle betrokken partijen binnen de organisatie. Ook de noodzaak om deze partijen van juiste informatie te voorzien door middel van rapportages kwam tijdens de case study naar voren. Dit vormt een cruciale voorwaarde om zowel het support van het management te behouden als betrokkenheid en bewustheid van de overige betrokken partijen. Om de doelstellingen van SAM te kunnen realiseren is dan ook meer nodig dan het implementeren van een aantal tools en processen. Het borgen van medewerking en ondersteuning vanuit diverse lagen van de organisatie is van groot belang.

Bij processen zoals lifecycle management is verder gebleken dat het creëren van continue traceerbaarheid van assets (closed loop) ertoe bijdragen dat organisaties 'in control' worden gebracht ten aanzien van hun software assets. Wanneer een organisatie beschikt over deze informatie kunnen inzichten opgedaan worden ten aanzien van licentieoptimalisatie en compliance gerelateerde vraagstukken.

De geïnterviewden gaven aan dat de doelstellingen in het framework als zodanig niet onhaalbaar voorkomen. De cultuur van de organisatie en de bereidwilligheid ten aanzien van SAM zullen bepalend zijn. Hier ligt dan ook een van de voornaamste doelstellingen van een Software Asset Manager, het continu behouden van support, bewustzijn en betrokkenheid van alle partijen. Door toevoegingen vanuit de case study voorziet het framework nu in deze aspecten.

6 Conclusie en beschouwing

6.1 Samenvatting hoofdstukken

Aanleiding voor dit onderzoek vormden de ervaringen die ik als software licentie auditor van diverse softwareleveranciers heb opgedaan tijdens mijn werkzaamheden. Het blijkt voor organisaties een grote uitdaging om in control te zijn ten aanzien van hun software assets en om het gebruik van software in overeenstemming te brengen en houden met de licentievoorwaarden. Buiten compliance vraagstukken zijn er andere risico's aan het gebruik van software binnen organisaties verbonden. Zo lopen organisaties financiële risico's als gevolg van bijvoorbeeld inefficiënt software gebruik of boetes naar aanleiding van licentie audit. Verder vormt verouderde of niet gemanagede software een beveiligingsrisico's en kan berichtgeving in de media ten aanzien van IT problematiek reputatieschade met zich meebrengen.

Om deze risico's het hoofd te kunnen bieden zijn in de vakliteratuur diverse best practices ten aanzien van SAM ontwikkeld. Doel van deze scriptie was om de doelstellingen van SAM te identificeren en te bepalen welke KSFen hiervoor aanwezig dienen te zijn om deze in de praktijk te kunnen realiseren. Door middel van een literatuurstudie en een case study wordt antwoord gegeven op de onderzoeksvraag.

In Hoofdstuk 2 is uiteengezet wat SAM precies inhoudt. In ITIL wordt SAM omschreven als alle infrastructuur en processen welke noodzakelijk zijn voor het effectief managen, controleren en beschermen van software bezittingen binnen een organisatie, door alle fasen van de software levenscyclus. Daarnaast is ingegaan op de vraag waarom SAM relevant is voor organisaties. Enerzijds bestaan er wettelijke verplichtingen voor organisaties zoals SOx wetgeving om interne controle te realiseren bij organisaties en dan voornamelijk ten aanzien van het gebruik van IT. Hiernaast ligt in de Nederlandse wetgeving een verplichting voor de accountant verankerd om in het kader van de jaarrekeningcontrole een uitspraak te doen over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Anderzijds kunnen er diverse risico's worden gemitigeerd en voordelen gerealiseerd. Deze voordelen zijn drieledig. Allereerst wordt SAM ingezet om risico's te managen zoals het reduceren van juridische- en financiële risico's als gevolg van overtreding van geldende licentievoorwaarden. Verder kan gebrek aan controle ten aanzien van softwaregebruik beveiligings- en dus continuïteitsrisico's met zich meebrengen. De tweede categorie van voordelen betreft het realiseren van kostenbesparingen. Kennis van beschikbare licenties en een actueel beeld van in gebruik zijnde software kan de onderhandelingspositie met softwareleveranciers aanzienlijk

verbeteren. Bovendien kan kennis ten aanzien van beschikbare licentievormen efficiënter gebruik van onderliggende hardware met zich meebrengen. De laatste categorie wordt gevormd door het realiseren van efficiencyvoordelen. Software kan beter gemanaged worden als er een duidelijk beeld is omtrent beschikbare licenties en behoefte vanuit de organisatie. Door optimalisatie van de hard- en software lifecycle kan nieuwe functionaliteit sneller beschikbaar worden gesteld.
In het literatuuronderzoek zijn drie best practices behandeld welke relevant zijn voor SAM en waarmee krachtens de theorie de doelstellingen van SAM gerealiseerd kunnen worden. CobiT is ontwikkeld om een IT-beheeromgeving gestructureerd in te kunnen richten. Gericht op het beschikbaar laten komen van relevante sturingsinformatie zodat de organisatie haar doelstellingen kan bereiken, is CobiT een stuk breder dan SAM. Toch vertonen meerdere processen binnen de CobiT domeinen raakvlakken met SAM. Gekeken is welke van deze processen als uitgangspunt kunnen dienen om de doelstellingen van SAM te realiseren. Verder is het conceptuele raamwerk ISO/IEC 19770-1 ten aanzien van SAM behandeld in Hoofdstuk 3. Aan de hand van een viertal Tiers kan op gestandaardiseerde wijze SAM geïmplementeerd worden; het hebben van betrouwbare data, het verbeteren van controle van het management, integratie met overige operationele bedrijfsprocessen en ten slotte het volledig conformeren aan de ISO norm. De toepasselijke procesgebieden om deze normen te kunnen bereiken zijn geanalyseerd. Ten slotte zijn de principes van ITIL behandeld, waar van een gefaseerde aanpak wordt uitgegaan voor een succesvolle implementatie. Het ontwikkelen van een visie, strategie en de communicatie binnen de organisatie hieromtrent, het implementeren en optimaliseren van beleid en werkprocessen en het creëren van een SAM database zijn in Hoofdstuk 3 behandeld.
Uiteindelijk is in Hoofdstuk 3 beargumenteerd dat de behandelde methodologieën allen handvatten bieden ten aanzien van SAM, maar dat gebruik van één enkele methodologie op zichzelf onvoldoende is om succesvol te kunnen implementeren. CobiT biedt weinig concrete handvatten en is meer gericht op controle van IT in brede zin. ISO biedt juist veel concrete procesvereisten ten aanzien van SAM, maar gaat niet in op de vraag hoe deze eisen gerealiseerd kunnen worden. Bovendien kunnen vraagtekens worden gezet bij de haalbaarheid van de vierde tier en de toegevoegde waarde hiervan. In ITIL wordt de focus gelegd op de implementatie op operationeel niveau en wordt dus wel ingegaan op de 'hoe' vraag. Deze literatuurstudie vormde de basis voor het theoretisch framework waar op basis van de best practices en eigen ervaringen KSFen zijn geïdentificeerd. Voor wat betreft de gekozen categorieën is aangesloten bij ISO, en is in afwijking van de frameworks specifiek de nadruk gelegd op het compliance aspect van softwaregebruik. Diverse factoren zijn geanalyseerd en uiteindelijk als KSF aangemerkt.
Het opgestelde framework heeft de input gevormd voor de interviews, waar een tweetal experts op SAM gebied gekeken hebben naar de volledigheid, juistheid en haalbaarheid van het framework. Uit deze interviews zijn diverse toevoegingen gekomen die hebben geleid tot nuancering van het framework. Uiteindelijk bleek dat er te weinig aandacht was voor cultuuraspecten zoals de continue noodzaak van support van het management en betrokkenheid en bewustzijn van verantwoordelijken. Andere toevoegingen richtten zich op informatieverschaffing. Welke informatie is relevant om voor te leggen aan betrokken partijen en het management? In Hoofdstuk 6 zijn deze aanpassingen verwerkt in het framework en zijn de KSFen uitgebreider toegelicht.

6.2 Beantwoording onderzoeksvragen

Om de hoofdvraag te kunnen beantwoorden zijn diverse deelvragen geformuleerd. Onderstaand volgen allereerst de antwoorden per deelvraag.

1. "Wat is SAM?"

SAM blijkt een zakelijke praktijk te zijn waarbij zowel mensen, processen als technologie betrokken zijn en is primair gericht op software welke de meeste impact heeft op de bedrijfsvoering van de organisatie. Omdat SAM een multidisciplinair proces is, zijn veelal meerdere afdelingen betrokken. SAM richt zich niet alleen op implementatie van processen, maar ook op continue verbetering hiervan. SAM omvat dan ook het

totale proces rondom het beheer en de optimalisatie van de planning, inkoop, implementatie, onderhoud en uitfasering van softwarepakketten binnen organisaties. Deze activiteiten dienen uiteindelijk te leiden tot een adequaat administratief beheer ten aanzien van de IT middelen van een organisatie.

2. "Wat zijn de doelstellingen van SAM?"
De doelstellingen van SAM kunnen uiteraard per organisatie verschillen, maar kunnen in drie categorieën van voordelen worden ondergebracht. Deze betreffen het management van risico's, het realiseren van kostenvoordelen en ten slotte kunnen diverse efficiencyvoordelen bewerkstelligd worden. Ten aanzien van risico management is het voorkomen van compliance issues (en hiermee mogelijk samenhangende reputatieschade) een van de voornaamste doelstellingen van SAM. Verder kunnen door SAM beveiligings- en dus continuïteitsrisico's gereduceerd worden. Kostenvoordelen kunnen gerealiseerd worden door een betere concurrentiepositie te bewerkstelligen. Bovendien kan de behoefte van een organisatie sneller in kaart worden gebracht omdat duidelijk is wat voor licenties er beschikbaar zijn en wat er is geïnstalleerd. Verder wordt overdeployment van software tegengegaan, kan hardware efficiënter worden ingezet waardoor een kostenreductie kan worden gerealiseerd. Ten slotte kunnen efficiencyvoordelen gerealiseerd worden door SAM. Op basis van juiste en volledige informatie kunnen kwalitatief betere beslissingen worden genomen, bovendien kan nieuwe functionaliteit sneller aan gebruikers beschikbaar worden gesteld.

3. "Welke kritische succesfactoren kunnen zowel in de theorie als praktijk worden geïdentificeerd?"
Om tot een succesvolle SAM implementatie te komen zijn op basis van de literatuurstudie en de interviews diverse KSFen geïdentificeerd. Het framework bestaat uit een aantal categorieën waarin processen zijn opgenomen welke op SAM van toepassing zijn. Een aantal KSFen zijn op meerdere categorieën van toepassing. Onderstaand volgt per KSF een korte toelichting en de toepasselijkheid per categorie.

- Budget -> besteedbaar bedrag dat aangewend wordt en voldoende is om de doelstellingen van SAM te realiseren.
  - Organizational Management Processes en Operations Management Processes and Interfaces
- SAM Capabilities -> De organisatie beschikt over medewerkers met voldoende capaciteiten ten aanzien van SAM.
  - Organizational Management Processes, SAM Inventory Processes en Life Cycle Process Interfaces (both hard- and software)
- Deze KSF is onderverdeeld in SAM Technical Capabilities en SAM Entitlement Capabilities.
  - SAM Technical Capabilities -> functioneel beheerders beschikken over kennis van configuraties van de software en zijn zich bewust van mogelijke implicaties hiervan ten aanzien van af te nemen licenties.
  - SAM Entitlement Capabilities -> kennis is beschikbaar ten aanzien van complexe gebruiksvoorwaarden van licenties en wat dit voor het gebruik van de software inhoudt. Focus ligt op het afnemen van de meest optimale licentievorm voor de organisatie
    - Software License Compliance
- SAM Resources -> Er is voldoende FTE aanwezig om de gestelde doelstellingen van SAM te kunnen realiseren
  - Organizational Management Processes, SAM Inventory Processes en Operations Management Processes and Interfaces
- Awareness Management en personeel -> Op structurele wijze borgen dat het management en andere betrokken partijen zich bewust zijn van het belang van SAM binnen de organisatie.
  - Organizational Management Processes
- Management Hierarchy -> Het management is in staat en bereidwillig om beslissingen af te dwingen indien dit noodzakelijk is voor het realiseren van de doelstellingen van SAM.
  - Organizational Management Processes

- Management Sponsorship -> Het management legt mandaten neer in de organisatie en ondersteunt de gemandateerde(n) op structurele basis
  - Organizational Management Processes
- Rapportages -> Stakeholders worden op de hoogte gehouden om bewustzijn ten aanzien van SAM te vergroten en support te behouden
  - Organizational Management Processes en SAM Inventory Processes
- SAM Databases -> Er zijn binnen de organisatie registraties aanwezig van het gebruik van software, aanwezige assets en beschikbare licenties. Bij deze informatiebronnen ligt de focus op juistheid van de informatie en het realiseren van een zo volledig mogelijke dekking binnen de organisatie.
  - SAM Inventory Processes, Software License Compliance en Life Cycle Process Interfaces (both hard- and software)
- Closed Loop -> Traceerbaarheid van software assets gedurende de aanwezigheid in de organisatie.
  - Software License Compliance en Life Cycle Process Interfaces (both hard- and software)

4. "Wat zijn de organisatorische voorwaarden om de kritische succesfactoren te realiseren/implementeren?"

Uit de interviews is gebleken dat de KSFen deels overlap vertonen met de organisatorische voorwaarden. Geïnterviewden gaven aan dat inspelen op de cultuur van de organisatie voorwaarde is om de KSFen te kunnen implementeren. Personen belast met implementatie dienen zich bewust te zijn van de cultuur binnen de organisatie. Zo zullen implementaties en veranderingen bij organisaties met een risicomijdende en passieve cultuur gericht op beheer anders verlopen dan bij jonge innovatiegerichte organisaties. Ongeacht de cultuur zal het bewustzijn van betrokken partijen moeten worden gestimuleerd. Werknemers belast met verantwoordelijkheden ten aanzien van SAM dienen op de hoogte te zijn van de 'waarom' vraag achter deze verantwoordelijkheid. Daarnaast dient geïnventariseerd te worden wat de bereidwilligheid binnen de organisatie is ten opzichte van de te stellen doelen ten aanzien van SAM. Wat is het ambitieniveau van de organisatie? Hierop dienen de doelstellingen te worden aangepast. Ten slotte zijn support vanuit het management en hiermee samenhangende verkregen mandaten voorwaarden om SAM te kunnen implementeren.

5. "Is het opgestelde framework in de praktijk toepasbaar?"

Als basis voor het framework zijn best practices van ISO en ITIL gebruikt. Er is gekeken naar een framework om praktische handvatten te kunnen bieden bij implementatie van SAM. Dit theoretisch kader is aangevuld door experts met ruime ervaring met SAM trajecten. Het framework biedt een overzicht van alle processen die binnen een organisatie door SAM geraakt kunnen worden. Hierbij zijn KSFen opgesteld die aanwezig dienen te zijn om de doelen van deze processen te kunnen realiseren. Het framework biedt een overzicht op basis waarvan concrete vervolgstappen kunnen worden genomen om de doelstellingen van SAM te realiseren.

6.3 Betekenis voor de IT-auditor

In de inleiding en in het eerste hoofdstuk van deze scriptie is benadrukt dat beursgenoteerde ondernemingen verplicht zijn om software te waarderen en in de balans op te nemen. Daarnaast ligt in het Burgerlijk Wetboek de wettelijke grondslag verankerd dat de accountant een uitspraak dient te doen over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking van een organisatie. In deze scriptie is uiteengezet dat met behulp van SAM software op een juiste en volledige wijze gewaardeerd kan worden en dat risico's ten aanzien van de continuïteit van een organisatie kunnen worden gemitigeerd. Hiermee lijkt de weg vrijgemaakt om tijdens de jaarrekeningcontrole aandacht uit te trekken voor licentiemanagement en in bredere zin SAM. Om na te gaan of dit in de praktijk ook gebeurt, en indien dit niet het

geval is waarom, is het in deze scriptie opgestelde framework aan een ervaren IT-auditor (hierna: Geïnterviewde C) voorgelegd. Geïnterviewde C beschikt over meer dan 40 jaar aan audit ervaring is tegenwoordig werkzaam bij IT Advisory Financial Services.
Op de vraag of er op dit moment tijdens de jaarrekeningcontrole aandacht wordt besteed aan vraagstukken met betrekking tot softwarelicenties en processen hieromtrent antwoordt Geïnterviewde C dat dit in principe niet gebeurt, tenzij hier specifieke aanleiding toe is. De IT werkzaamheden tijdens een jaarrekeningcontrole richten zich primair op de betrouwbaarheid van primaire processen binnen de organisatie en andere operationele vraagstukken. Hierbij wordt de nadruk gelegd op processen die van directe invloed zijn op de primaire applicaties van de organisatie. Oftewel uitsluitend de General IT Controls die ten grondslag liggen aan de financiële applicaties worden op betrouwbaarheid en continuïteit getoetst. Het waarderingsvraagstuk van de software wordt in principe aan de accountant zelf overgelaten, waarbij de hieraan verbonden risico's waarschijnlijk niet als hoog zullen worden aangemerkt. Dit zou bijvoorbeeld anders kunnen worden wanneer een audit van een grote softwareleverancier is aangekondigd of wanneer hier bevindingen uit voortgekomen zijn welke materiële gevolgen kunnen hebben. De accountant zal in het laatste geval hier meer aandacht aan besteden, deze dient immers te voorkomen dat er een post goedgekeurd wordt met eventuele materiële gevolgen. Pas op het moment dat er een concreet financieel belang aanwezig is zal naar verwachting de aandacht voor softwarelicenties en SAM toenemen.
Met betrekking tot continuïteits- en beveiliging gerelateerde vraagstukken stelt Geïnterviewde C dat in het kader van de jaarrekeningcontrole aandacht wordt besteed aan change management en patch-management processen binnen de organisatie. Om de continuïteit en beveiliging immers te kunnen waarborgen dient vastgesteld te worden of hiertoe relevante beheersmaatregelen zijn genomen. Vanuit beveiligingsoogpunt wordt gekeken naar de in gebruik zijnde versies van de applicaties welke object van onderzoek zijn, maar niet of hier organisatie brede aandacht voor is en procedures voor zijn.
Geconfronteerd met de mogelijke financiële gevolgen van een licentie audit geeft Geïnterviewde C aan hier niet bekend mee te zijn en dat dit voor veel organisaties waarschijnlijk materiële gevolgen met zich mee zou kunnen brengen en dat de accountant hier meer aandacht aan zou moeten besteden. Omdat een accountant echter vaak terugkijkt en primair een uitspraak doet over de betrouwbaarheid van de financiële rapportage van het voorgaande jaar ligt het niet voor de hand dat uitgebreid aandacht zal worden besteed aan de effectiviteit en optimalisatie van processen rondom softwaregebruik. Pas wanneer negatieve financiële gevolgen (en reputatieschade) reëel worden zal de accountant op onderzoek uit gaan, maar dan primair gericht om deze financiële gevolgen te kunnen waarderen. Ten aanzien van beveiligingsvraagstukken en SAM geeft Geïnterviewde C aan dat, indien hiertoe aanleiding is, de werkzaamheden met betrekking tot versie- en patchmanagement uitgebreid kunnen worden om zodoende vast te kunnen stellen dat beveiligingsvraagstukken met betrekking tot versiebeheer kunnen worden geadresseerd. Dit laat echter onverlet dat er nog steeds machines binnen een organisatie aanwezig kunnen zijn die niet gemonitord worden, en dus niet geüpdatet. Omdat deze mogelijke machines niet gemanaged worden zullen deze geen object van onderzoek zijn van de jaarrekeningcontrole.
Geïnterviewde C is er voorstander van om tijdens de jaarrekeningcontrole aandacht te besteden aan licentievraagstukken om vast te stellen of dit een aandachtspunt binnen de organisatie is. Indien dit niet het geval is, zou de accountant hier eventueel melding van kunnen maken in de management letter.

Sap Process Control in Practice

Sylvester van der Giesen
D.A. Kimball B.B.A.

	
Sylvester van der Giesen MSc is a manager at KPMG Advisory. He has been with KPMG since 2012 and focuses on the intersection between business and IT with a strong focus on SAP products. In this role he has grown as a subject matter expert in SAP GRC Process Control and Risk Management.	D.A. Kimball B.B.A. is a manager at KPMG Advisory. He has been with KPMG for seven years, with a focus on security, risk and controls. He has developed as a SAP GRC specialist and currently works for KPMG Netherlands through an exchange program with the Dallas office from KPMG Advisory US.

1 Introduction

There are numerous tools and systems available that enable organizations to gain control and comply to rules and regulations. Examples of these tools are BWise, MetricStream and SAP Process Control. These tools and systems help companies to document their processes, risks and controls, capture evidence of executed controls, monitor and follow up on issues and report on the compliance status of their organization. Many companies using SAP as their core ERP system tend to choose SAP GRC as their risk and control monitoring system. Therefore, we will focus on SAP Process Control and describe its main capabilities and functionalities, implementation considerations and how custom reporting can be leveraged.
In an ever increasing complex and regulated business environment, organizations are faced with challenges on how best to manage internal controls and compliance. Despite the recognition that efficiencies could be gained through a more automated control model, many companies are relying on manual processes. Leading companies recognize the importance and urgency to stay ahead of today's compliance curve and keep pace with changing regulatory and audit requirements.
Governance, risk, and compliance (GRC) has become a top executive priority, but many organizations are struggling to manage and control risk effectively today. The 'three lines of defense' operating model for managing risk provides a framework that allows organizations to set up their risk and compliance organization. The following lines are defined in the three lines of defense model (see Figure 1):

1 the 1st line is business operations management;
2 the 2nd line includes risk management, compliance, security, and legal departments;
3 the 3rd line is the independent internal audit function.

Figure 1. Three lines of defense model

There are numerous tools and systems available in the market that enable organizations to gain control and comply to rules and regulations. Examples of these tools are BWise, MetricStream and SAP Process Control (see Lamberiks, 2017) article on trending topics in GRC tools in this Compact edition). These tools and systems help companies to document their processes, risks and controls, capture evidence of executed controls, monitor and follow up on issues and report on the compliance status of their organization. Many companies using SAP as their core ERP system tend to choose SAP GRC as their risk and control monitoring system.
Therefore, this article will focus on SAP Process Control and describe its main capabilities and functionalities, implementation considerations and how custom reporting can be leveraged. At the end, we will discuss the effects of two practical implementations of SAP Process Control.

2 What is SAP Process Control?

SAP Process Control (PC) is an enterprise software solution which can be used by organizations to manage their compliance processes more effectively and realize the value of a centralized model.
Data forms, workflows, reminders and escalations, certifications, and the use of interactive reports support members of business process teams, internal control and internal audit to carrying out their individual compliance activities. Process Control provides a centralized controls hub in which testing, certifications and policies, monitoring and documentation can take place.
Process Control is a key part of SAP's GRC software, sitting alongside SAP Risk Management, which enables an organization to define its enterprise risk and responses to those risks and SAP GRC Access Control, which assists in detecting, remediating, and ultimately preventing access risk violations. Although not a requirement for implementation, Process Control can be integrated with these two modules to provide added value to customers of SAP GRC.

3 Process Control key functionality

SAP Process Control provides the following core functionalities (see Figure 2):

1 Provides documentation of both centralized and local control catalogs, alignment of compliance initiatives and efficient management of risks and controls through workflow functionality.
2 Supports scoping through risk assessments and materiality analysis as well as the planning of control testing.
3 Supports the design and test of the operating effectiveness of controls with online or offline workflow functionality and consistently registers test evidence and issues found from testing. Control testing can be performed manually, semi-automated and fully automated.
4 Enables the documentation of control deficiencies and issues and provides reporting capabilities to track and correct deficiencies (i.e. re-evaluations).
5 Leverages sign-off and periodic disclosure survey functionality to formalize management approvals which includes issue tracking and deficiency remediation.
6 Allows a full audit-trail and log of performed test steps, including documented sign-offs to allow for an independent control audit.

Figure 2. Core functionalities of SAP Process Control

In practice, some auditors at organizations using Process Control have leveraged the controls description and evidence in Process Control for their (IT) audit procedures. So far, the risk assessment and materiality analysis functionality in Process Control have not been used for this financial statement audit purpose.
SAP GRC Process Control can also perform continuous control monitoring, including monitoring the segregation of duties and critical risks defined in SAP Access Control. Controls can be monitored at a specified frequency (weekly, monthly, etc.) and results can be automatically sent to appropriate control owners.

4 Considerations for implementing SAP Process Control

When implementing Process Control there are several areas to focus on, including master data setup and workflow considerations. Automated control setup and reporting are summarized.
Besides these focus areas for SAP Process Control it is also very important to consider the use of SAP Access Control and SAP Risk Management and the integration of the various modules in the GRC suite. When all three modules are set up, there will be shared data and integrated functionalities which may need additional attention during the setup of the system.

4.1 Master data setup

Process Control master data has two important components: the organization hierarchy and the control library. When setting up the organization hierarchy there are two key questions that need to be answered:

1 What model will be used to define hierarchies and who should be involved? If multiple GRC components are being installed (the organization hierarchy can be shared by Access Control and Risk Management), multiple teams may need to be involved in the setup of the organizations.
2 How should the organization report on compliance? This could be on a company code level, line of business, or by region. In some cases, multiple reporting requirements need to be integrated and reflected in the organizational hierarchy. E.g. some organizations require lower level reporting and tend to set up every company code as an organization, whereas other organizations need more high-level reporting and set up reporting entities (a group of countries or company codes) as their organizations.

It is important to make decisions around the control framework before loading the control library into Process Control. Here are some aspects to consider:

1 In case there are multiple control frameworks in the organization, which one should be loaded to the system? Should they be harmonized, or should they be separate? What kind of information is most important and should be included in the system, and which information could be discarded?
2 How to test shared service controls? Will a shared service organization be used in the system or are the individual controls tested and documented by control performers from a shared service center?
3 All controls need to be assigned to a subprocess, without the subprocesses it is not possible to maintain a control library in Process Control.
4 Is there a clear distinction as to which controls are performed in which organizational unit? This is necessary for the control to organization mapping.
5 Will it be required to document account groups, financial assertions and risks covered by the control and control objectives? Process Control has master data available for each of these items that can be setup. This is required if scoping is performed in SAP Process Control.

The master data is the foundation of the system. When (Master) Data Management is not thought through or set up correctly and according to the company needs, there could be an impact on reporting and efficiency of the functionalities that are used. If framework integration is not performed properly this could even lead to duplicate controls being tested.

4.2 Workflow use cases

The second important area of interest during an implementation is around workflow. The first question to ask here is: 'What does the organization's compliance process look like, how are controls to be tested, and should this be documented?', since it makes sense to only implement workflows that will benefit the organization. Furthermore, it is important to bring all the relevant stakeholders together and agree on the owners of the various workflow tasks and which areas can and cannot be customized. It is also important to agree upon the degree of notifications and reminders that are needed. If users get too many emails, the intent of the emails could get lost and users may end up ignoring them.

Once the testing cycles have started and the system starts being used, it is important to have an administrator to monitor all incoming tests and if necessary reroute, close or even delete them from the system. This must be done with the utmost care and should only be performed by experienced Process Control administrators.

4.3 Automated controls

SAP Process Control can perform semi and fully automated testing of controls. The SAP GRC module retrieves the settings from the target system and analyses reports or system settings and validates these against set business rules to determine whether the settings comply or not.

When setting up automated controls, there are different types of controls that can be identified: application controls, master data controls and transactional controls. Even though Process Control offers various integration scenarios, the key is to keep it simple upfront and focus on configuration and master data controls to achieve minimum setup difficulty. The different types are depicted in Figure 3.

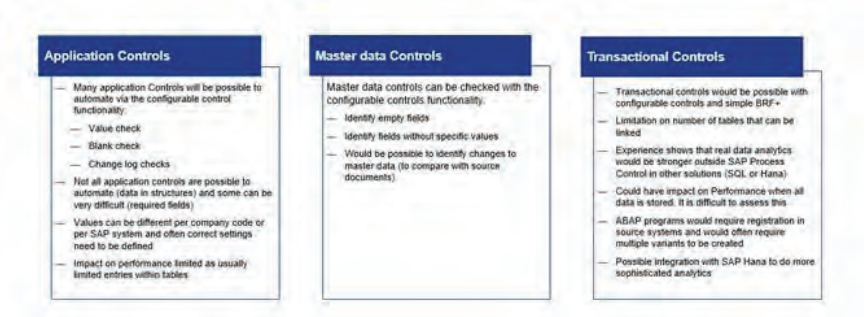


Figure 3. Control types for automation

The most important integration scenarios to cover these types of controls are:

- The ABAP (Standard SAP Report) integration scenario (e.g. providing control performers with the RSUSR003 Report). The added value of ABAP report controls is the (workflow) support it provides to internal control staff for retrieving the right data from the various SAP systems and delivering it to the appropriate mailbox for further analysis.
- The configurable controls scenario (e.g. check whether tolerance limits are set). The configuration controls are stronger than the other two types, on a daily basis and based on a change log that the customized settings in SAP can be verified.
- The HANA (SAP Advanced analytics platform) integration scenario (e.g. perform advanced analytics to find potential duplicate invoices). The integration with Process Control is to relate the identified exceptions to a control, and assign such controls to the right staff.

While setting up automated controls it is essential that the controls are pre-tested in the acceptance environment and that stakeholders as well as control owners are aware of the potential issues that will be raised as outcomes when controls like these are automatically tested.

4.4 Reporting

The topic of reporting is often forgotten during Process Control implementations, despite its utmost importance. In order to get most value out of the reporting the key is to define the different audiences and only provide relevant reports to each audience. When all reports are available to everyone, this could become an overkill of reporting possibilities and confuse the end users.
During an implementation of SAP Process Control reporting requirements should be gathered up front so that they can be used as a guideline throughout the project. As mentioned before, the organization structure plays a vital role in the system and will also impact the way reports can be used and visualized.
If the standard reporting capabilities in Process Control are insufficient for an organization's management reporting (for instance due to tactical information needs), external dashboards could be created based on relevant Process Control tables. In order to do this, technical knowledge of the system and its data model is required.

5 Master data components and considerations

A key differentiator for SAP Process Control is the shared catalog of master data that comes from a multi-compliance framework. SAP Process Control allows companies to manage requirements from different regulations and mandates (SOX, JSOX, 8th EU Directive, GDPR, FCPA, etc.) from one central place. Test results of a control will be applicable for multiple regulations, which reduces the overall test effort which would result in cost savings. Much of the master data can be shared between the various GRC modules: Process Control, Access Control and Risk Management. Some examples for this shared data are organizational data, mitigating controls, risks for SAP Risk Management and SAP Process Control.
Both central master data (applicable to the entire company) and local master data (organization dependent) are necessary to setup:

Central master data:
- Organizational Structure
- Risk Library
- Control Objectives
- Account Groups and Assertion
- Central Control Library
- Regulations and Requirement
- Policies
- Indirect Entity-Level Controls

Local master data:
- Organization-dependent Subprocesses
- Organization-dependent Control
- Organization-dependent Policies
- Organization-dependent Indirect Entity-Level Controls

5.1 Organizations

The organization structure is the central common master data entity in SAP GRC. The organization structure can be shared among SAP Risk Management, SAP Process Control and SAP Access Control. Often the structure of the company codes in SAP can be used, where company codes are grouped in countries. However, sometimes the reporting entities are not similar to company codes or structures and alternative structures need to be developed, such as by functional area or business unit.

Organization Structure Setup

Companies need to determine how they will arrange their organization hierarchy. It is important that this structure is well considered before building this master data in SAP PC. Consider the following:

1 What model will be used to define hierarchies and who should be involved? If multiple GRC components are being installed (the organization hierarchy is shared by Access Control and Risk Management), multiple teams might need to be involved in the setup of the organizations.

2 Additionally, the key question is how the organization will report on compliance. Is that on a company code level, a line of business level or perhaps a regional level? In some cases, multiple of these reporting requirements need to be adhered to, and need to be reflected in the organizational hierarchy.

Organizations can be grouped as nodes in an organization hierarchy, with sub-nodes such as legal entities, plans, profit centers or divisions.

5.2 Central process hierarchy

Defining processes and subprocesses is also an essential step in master data setup. A process refers to a set of activities relating to a specific function in an organization's operations, such as purchasing. A subprocess refers to a subset of activities within a business process, such as accounts payable within purchasing. Controls are created under subprocesses and are assigned to compliance areas/regulations. A process node can have any level of nested child process nodes, or a single child level of a subprocess. A subprocess can only have control as a child (see Figure 4).

Figure 4. Process hierarchy

The entire business process hierarchy exists mainly to provide context for the control; while the amount of information that can be maintained at the process and subprocess level is limited. The control is the main SAP Process Control master data type through which much of SAP Process Control functionality is presented.

Master data creation and customizations

There are many dependencies when it comes to Process Control master data. It is recommended to create the objects in the following order:

1 Regulations;
2 Control Objectives and Risks;
3 Process, Subprocesses and Controls;
4 Organizations.

Notes:

1 Once all the objects are created, master data assignments can be performed, such as assigning sub-processes to organizations.
2 Multiple organizational views can be created if separate master data is desired for Access Control, Process Control or Risk Management.
3 Field based configuration can be customized to hide field and/or allow 'local' changes to a field. Attribute values can also be edited, which results in changed contents of fields in the controls screen.

Audit-trail

It is important to note that nearly all of SAP Process Control master data has effective dates (from and to). This helps to drive alignment with regulations, organizational structures, business process models, controls, monitoring rules, test plans, assessments, and surveys that change over time.

Master data upload

The MDUG tool in SAP Process Control allows administrators to mass upload data for PC Risk Management from a MS Excel Sheet. This enables customers to capture all their master data in a single place, which makes reviews and signoffs more convenient.
Note: the MDUG template can often take multiple reiterations in order to upload without errors as SAP checks for multiple items, such as mandatory fields. Refer to the SLG1 logs for insight into upload errors.

6 Workflow capabilities in SAP Process Control

6.1 Surveys and test plans

When workflows are to be sent out, there need to be surveys or test plans that guide the user in performing their task.
Surveys contain several questions which need to be answered by the user in order to complete the task. The survey questions are set up by the organization itself and can have multiple answer types. The following answer types are supported:

- Rating: this provides rating buttons from 1 to 5;
- Yes/No/NA;
- Choice: you can define your own answers;
- Text: free text field.

The surveys can be configured in a way where comments are required once an answer is selected. The surveys need to be setup for each workflow (e.g. one for self-assessments, one for control design assessments, etc.). When the workflow is planned the survey that needs to be used is selected. Based on this, the workflow task (both online and offline) will be created with questions from the selected survey.
Test plans are slightly more elaborate and need to be created for each control. The test plan includes steps that need to be performed in order to perform the independent test, including the sample size and sampling method. The test plans need to be assigned to controls in the business process hierarchy. When a test of an effectiveness workflow is sent to the users, the test plan assigned to the control is represented in the task. The user that performs the test plan then needs to execute and pass or fail each step. When this is done a final pass or fail needs to be selected for the entire test task.

Test plan usage

If test plans are maintained for each control: they also need to be maintained in the system for each control e.g. if there are 300 controls, there will also be 300 test plans, all with multiple steps. It can be beneficial to create one generic test plan with the possibility to add control specific attachments.

A manual control performance plan also needs to be maintained for each control for the manual control performance workflow. This allows the control performance steps to be assigned to multiple testers, enabling shared ownership for performing controls and documenting evidence.

6.2 Available workflows

To support organizations in carrying out their compliance with regulations and frameworks, Process Control provides several default workflows to capture execution of control assessments and control tests. Table 1 shows the various workflows that are available and how they can be used and customized within a business context.

Workflow	Use Case
Perform Control Risk Assessment	The Control Risk Assessment is typically used during the scoping phase and is used to determine the risk around a control failure. When the risk of failure of the control is higher this impacts the number of samples that need to be selected for independent testing.
Perform Sub-process Design Assessment	Sub-process Design Assessments are used to inquire sub-process owners about their sub-processes that are set up in the system and whether these are still aligned with the actual sub-processes that are executed in the business. This is typically performed annually or bi-annually.
Perform Control Design Assessment	Control Design Assessments exist to periodically check control validity. Inquiries are sent to control owners typically on an annual or semi-annual basis to ensure the controls in the system are accurate and align with the business.
Manual Control Performance	The manual control performance workflow is sent out to control performers and is meant to document all steps performed to complete the control execution, including filing all evidence of these steps in the workflow. This provides additional visibility on the execution of control at a detailed level.
Perform Self-Assessment	Self-Assessments are used to gather information on the control performance over a certain period of time by sending a survey with questions about the control and the execution of the control to the control owner.
Test Control Effectiveness	The test of effectiveness workflows is used to perform an independent test (test performed by somebody who is not the direct owner of the control) and determine whether the control was effective over a certain period of time by taking a sample of the actual control execution. The effectiveness can then be assessed in multiple ways such as reviewing the samples or re-performing the samples.
Perform Control Disclosure Survey	By sending out a Control Disclosure Survey a person who is responsible for a certain number of controls is asked to disclose that they are aware of their controls performance and any open issues. This will lead to increased accountability and auditability, providing management with better comfort with regard to their controls.
Perform Sub-process Disclosure Survey	A Sub-process Disclosure Survey is sent out to specific sub-process owners to ensure that they are aware of sub-process performance and any open known issues. This leads to increased accountability and auditability, providing management with better comfort with regard to their controls.
Perform Organization Disclosure Survey	An Organization Disclosure Survey is sent out specific organization leaders to ensure that they are aware of controls performance and any open known issues. This will lead to increased accountability and auditability, providing management with better comfort with regard to their controls.
Perform Indirect Entity-Level Control Assessment	The assessment for entity-level controls is similar to the assessment of a regular control and is used to inform the owner of the entity-level control about the performance of the control over a certain period of time.
Test of Indirect Entity-Level Control Effectiveness	The test of effectiveness for entity-level controls are used to perform an independent test (test performed by somebody who is not the direct owner of the entity-level control) and determine whether the entity-level control was effective over a certain period of time.
Perform Aggregation of Deficiencies	Aggregation of Deficiencies is typically used at the end of a fiscal year or other reporting period to provide higher management with a grouped view on failed controls. A deficiency level is set for every failed control, so deficiencies can be grouped according to their levels. When this activity is performed, management is better informed to determine compliance gaps from the aggregated view.
Perform Sign-Off	The sign-off is similar to the mentioned disclosure surveys and is used to provide higher management with better confidence on the compliance status and open issues. In contrast with the disclosure surveys the sign-off functionality 'freezes' the system to reproduce a period or timeframe.

Table 1. Available workflows and corresponding user cases

Use of workflow types

Although SAP Process Control contains many different assessment and test types, it is recommended to carefully review the user case for the different workflows in the organization, and not to implement workflows that will never be used.

For all the workflows where an effectiveness rating is provided there is a built-in check which forces the user to create an issue in case the control assessment or test or sub-process assessment failed. When the issue is created, an issue workflow is automatically started. The issue workflow can be leveraged to follow up on the issue and take corrective and preventive actions or start a remediation workflow.

6.2 Workflow setup options

As not every organization has exactly the same compliance monitoring processes, SAP Process Control can be customized to better fit the needs of an organization. For all assessment and test workflows a review step can be added in the workflow. The system can also be set up in such a manner that a review step is

automatically skipped, based on the rating of the assessment or test (e.g. when the control assessment or test was rated effective the review step will be skipped).

Different flows in different entities
When the global system is set up to trigger a review for every task performed, but this is not mandatory for all entities within the company, there is a setting in the master data which allows to defer from the standard workflow per organization or per subprocess.

To ensure that stakeholders are aware of the tasks that they need to perform, the system can send automatic notifications, reminders and escalations via email. A notification will be sent to the user that needs to perform a task when the task is created, a reminder is sent to the user some time before the deadline and an escalation is sent to the accountable person just before, or even slightly after the deadline.

There should not be an overkill of email
When notifications, reminders and escalations are all active, a lot of email will be generated. When too many emails are generated, it becomes an overkill and people will get annoyed and set up email rules to automatically reroute or even delete the email from SAP Process Control out of their inbox.

To make the workflows more accessible, SAP Process Control also enables offline processing, making use of Adobe Smart forms. By making use of this functionality, all workflow tasks that are normally performed in the Process Control system can now be performed using interactive PDF files and regular email. When making use of interactive PDF forms, it is important to monitor the system upon creation of the PDF's, and that PDF's are correctly sent out.

Monitoring the incoming tasks
If the offline Adobe forms are used, it may be beneficial to monitor the process more closely. The following transactions can be helpful:
- ST22: to troubleshoot short dumps;
- SLG1: to identify possible inbound emails that have not been correctly processed;
- SOST: to monitor outbound and inbound email messages.

6.3 Monitoring workflows
When workflows are sent out to the internal control community, it is vital to monitor whether workflows are also closed before the set deadline. SAP Process Control provides a standard functionality which shows an overview of all open tasks, which user currently needs to act on the tasks and whether the task is overdue or not. This overview can be found in the 'planner monitor'.
When workflow tasks are stuck, it may be necessary to push, reroute or even delete existing workflow tasks.

Workflow administration
Deleting existing workflows must be performed with utmost care. If this is not done properly, workflow tasks could be damaged, or the information of other or all workflows could be removed. When not performed correctly, there can be a large impact on compliance evidence.

7 Continuous control monitoring

SAP provides functionality to automatically test controls in SAP or in other SAP applications. This can provide great value to organizations and increase efficiencies around control testing. Automated controls

often receive a high level of interest from auditors. If they can rely on automated controls, there is a potential that their workload will significantly decrease. There are different kinds of integration scenarios possible. In this article, we will discuss the following:

- the ABAP integration scenario;
- the configurable controls scenario;
- the HANA integration scenario.

Continuous control monitoring is set up by connecting the SAP GRC system to other SAP and non-SAP systems. For SAP systems a RFC connection can be leveraged and for non-SAP systems a special third-party connector or an offline connector (with flat files) is necessary. An example of this is shown in Figure 5.

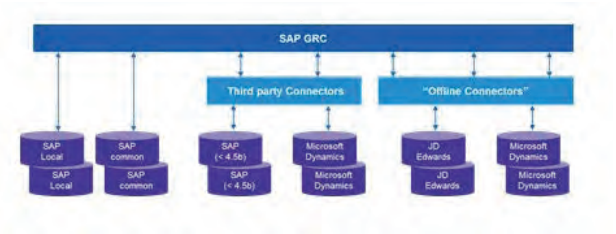


Figure 5. Connection types

Automated monitoring requirements

In order to allow automated monitoring in SAP systems, the relevant SAP plugins (GRCFND_A and GRCPIERP) need to be installed in the target SAP system. Additionally a RFC connection needs to be created and a user with the proper authorizations should be available.

Once GRC is connected to other systems, data sources can be created in Process Control. When creating a data source in SAP Process Control, it is possible to link up to five tables together. In order to make use of the programmed or ABAP report scenario, a program or ABAP report needs to be set up for consumption in the SAP target system.

Automated controls: ABAP reports

In the case of the ABAP integration scenarios, keep in mind that the ABAP program that needs to be run, needs to be registered in the ABAP Source system with its variant. The variant can be used to make distinctions between organizational entities in SAP. In some cases, additional variants need to be created as part of a SAP PC implementation.

When setting up configurable controls for SAP systems a connection is made to the target system to gather data directly from tables. When the data source has been created (e.g. connection to T001 table) a business rule needs to be set up in SAP Process Control. In the business rule the logic is provided for the system to determine whether values found in the data source are in line with the control (effective) or are not correctly set (ineffective). Based on this logic the system can automatically test controls, e.g. when the company code in table T001 is not set to productive (field XPROD equals X), then the control fails.

Automated monitoring

A configurable control with a daily frequency only checks a certain value once a day. If people know at what time the value is checked, they can still get past the control by changing the value just before and just after the check is done. To prevent this a change log check can be set up. The change log check is similar to a normal configuration control, but provides the changes to the value over a set period of time.

By doing both the regular value check and the change log check it is ensured that the control is effective and has been effective during a set period. This is often the confidence that auditors are interested in.

Many organizations want to make use of the automated controls functionality to monitor transactional or master data controls. However, SAP process control can particularly be used to monitor and test the controls that have been implemented in the SAP application itself, so-called application controls. The SAP configurable control functionality can be used for this by performing blank checks (no data has been maintained for specific fields), value checks (values below or above certain thresholds) and change log checks. It is not easy to check for duplicate values within a data source.

Automated monitoring
A change log check is possible when the change logs on tables have been activated and when the specific table has been flagged to log changes. The change log on a table can be switched on in the target systems via transaction code SE15.

In some cases, a combination of different kinds of controls can be used to monitor the actual implementation of the control in the application (required fields within vendor master data) and the effectiveness of the control by monitoring actual data in the system (identifying where required fields have not been populated within master data).

Configurable controls monitoring: what is the real control?
The automated control functionality supports the testing of controls, but it is important to understand what the actual control is. A useful example is the duplicate invoice check. There are multiple settings required in order to enable the duplicate invoice check. These settings are:
- the duplicate vendor check in vendor master data (set as a required field LFA1);
- the warning message that a duplicate invoice has been posted (SAP Configuration – Change Message Control);
- the setting that the systems need to check on additional fields (transaction code OMRDC).

There are three controls that are required to prevent duplicate invoices from being posted. However, the vendor account number is always considered in these checks. Nonetheless, most companies still have many duplicate vendor master data records or make use of one-time vendors, which would allow the possibility to post a duplicate invoice line in the system (or typos made in the actual posting reference number).

A new upcoming solution for control automation is the HANA integration scenario. When there is a connection from the SAP HANA System to the SAP Process Control system, data sources can be set up against SAP HANA calculation view. When this connection is in place a whole new level of analytics and exception reporting can be done with SAP Process Control, by leveraging the powerful and advanced analytical capabilities of SAP HANA.

HANA integration
SAP advises the use of scripted calculation views in SAP HANA to connect to SAP Process Control, even though both scripted and graphical views can be used.
Note: not all field types are supported in SAP Process Control, e.g. timestamp fields are not supported.

8 Reporting and dashboarding

Throughout the year, and especially at the end of a compliance cycle, every organization wants to know how they stand against their controls. Thankfully, SAP Process Control comes with many different reports

that can help organizations see where they stand. In this section, the most relevant reports for each section are described and the possibilities of customized dashboards are explained.

8.1 Master data reports

Reports in the master data section are mostly used to check the integrity and completeness of the master data that has been set up. All changes to master data are automatically captured and can also be reported. The reports are shown in Table 2.

Report	Audience	What is the report about?
Risk & Control Matrix	Compliance officer, Auditor	Overview of processes and controls that are assigned to organizations
Risk Coverage	Compliance officer, Auditor	Overview of risks per organization and whether these are covered by any assigned controls
Organization and Process Structure	Compliance officer, Auditor	Hierarchical overview of organizations and their assigned controls
Change log	Auditor	Comparison of master data between two defined periods. This provides a direct insight in changes over a period. This report is highly valued by auditors
Audit Log	Auditor	List of all changes to central or local master data

Table 2. Master data reports

8.2 Automated control reports

Automated controls often receive a high level of interest from auditors. If they can rely on automated controls, there is a potential that their workload will significantly decrease. The reports in Table 3 can be used by auditors.

Report	Audience	What is the report about?
Data source Business Rule Assignment	Auditor	Overview of data sources, the business rules that are assigned against it and the status of the data sources and business rules
Automated control Business Rule Assignment	Auditor	Overview of automated controls in the system and which business rules are assigned against them.
Control Monitoring History with Ratings	Control owners, compliance officer, auditor	Results of control monitoring control tasks and the rating. This provides both the deficient and adequate automated monitoring controls.
Monitoring Issue Status	Compliance officer, auditor	All issues raised by the automated monitoring process, it provides quick insights into the number of issues and whether actions have been taken.
Monitoring Remediation Status	Compliance officer, auditor	All remediation plans that have been created after issues that have been raised based on automated monitoring tasks.

Table 3. Automated control reports

Changes to business rules

To report on changes to business rules, the 'Audit Log' report in the master data section can be used to report only on business rules. This shows all changes to business rules over the selected period.

8.3 Workflow-related reports

The workflow-related reports are used to show the actual compliance status and progress. In the end, compliance is based on the number of controls that are assessed or tested with a positive rating. The reports that provide insights for this are in the 'Assessments' section of the application. The reports in Table 4 are of interest.

Report	Audience	What is the report about?
Evaluation Results by Organization	Compliance officer, organization owner, auditor	Overview of workflows (Self-Assessment, Control Design Assessment, Sub-process Design Assessment, Test of Effectiveness), linked to a hierarchical view of the organization structure.
Assessment Survey Details	Compliance officer, control owner, auditor	Overview of workflows (Self-Assessment, Control Design Assessment, Sub-process Design Assessment, entity-level control assessments) including the option to add all questions, answers and comments from the survey.
Test Status by Organization	Higher Management, Compliance officer, organization owner, auditor	High level overview per organization of the number of assigned controls, the number of Control Design Assessments performed (including percentage failed), the number of Control Self-Assessments Performed (including percentage failed) and the number of Tests of Effectiveness performed (including percentage failed).
Manual Control Performance Details	Control owner, auditor	Overview of executed control performance tasks including the detailed steps performed and the comments on them
Issue Status	Compliance officer, Auditor	Overview of all created issues in various workflows including their follow up actions.

Table 4. Workflow-related reports

8.4 Dashboarding

By default, SAP Process Control provides several standard dashboard reports. Even though this dashboard can show results for several workflow types (e.g. Assessments, Tests) and even subtypes (e.g. Control Design Assessment, Self-Assessment), its functionality is limited and does not provide proper information for senior management.

Additionally, SAP Process Control now provides functionalities called 'side panel' and 'entry page'. When the side panel is activated, an additional panel is opened, for instance next to the organization structure. Upon selecting an organization, the side panel will show a small dashboard with assessment or test details and issue details for the controls in that organization. Such a feature can be useful for end users navigating the system. The entry page can be set up per role and can be used to create an entry page with relevant insights into compliance status, status of control assessments, control tests and issues. This entry page can be customized as part of the implementation.

Custom dashboards can also be developed based on data from the system. When creating custom dashboards, the following aspects must be carefully considered:

- Data extraction from (other) systems can be performed in multiple ways (e.g. manual extraction, replication to a HANA system).
- The data must be modeled, so it can be leveraged for a dashboard (there is logic that needs to be applied).
- Organizations must define their own KPIs. Without proper KPIs, the value gained from the dashboards is limited.
- Authorizations are different in dashboards: system authorizations are not automatically captured and applied. E.g. if a user is authorized to only display controls for one organization in the GRC system, then this will not be automatically captured in a dashboard as well. This may require separate dashboards or advanced authorizations for the dashboard if this is possible.

Relevant tables

The master data in SAP Process Control is captured in HRP* tables (e.g. all object names are stored in HRP1000, control details are stored in HRP5304). Other information, such as workflow information, is mainly stored in tables starting with GRPC* (e.g. GRPCCASEAS contains information about assessment workflows).

When custom dashboards are created, organizations are free to set up the reporting according to their own interest and level of detail. It is often easier to gain higher level insights and compare different parts of the organization using custom dashboards. Figure 6 shows a possible custom dashboard.

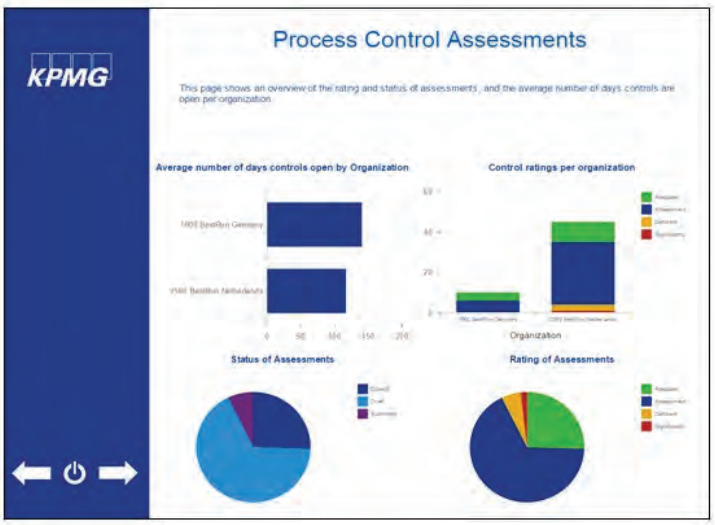


Figure 6. Dashboard example

9 Case studies

In this section, we have described how two organizations are using SAP Process Control.

9.1 Case 1: from quarterly parameter checks to continuous monitoring

Context
A large multinational with over 10 Billion in Revenue has over 20 centralized SAP systems. For each of these SAP systems, the (security) parameter settings need to be monitored in order to adhere to their baseline. The security baseline covers over 100 (security) parameter settings in SAP.

Situation prior to using SAP Process Control
Before SAP Process Control was used, the security settings for each central SAP system were reviewed each quarter. The review was performed manually and documented by creating screenshots of each relevant system setting. These documents were over 100 pages per SAP system. The follow-up on findings of these reviews were limited and rarely documented due to the manually intensive process. If changes occurred during the quarter (eg. a setting was changed to an incorrect value and changed back to the correct value just before the review), there was no possibility to identify these potentially undermining changes.

Situation after
By using continuous monitoring via SAP Process Control, the system parameters are now monitored on a weekly or monthly basis (dependent on the risk profile) and on top of that, all changes to parameters are identified and reported. Furthermore, the monitoring is now exception-based. This means that parameters

which are set to the correct values are reported as effective, whereas parameters that are set to an incorrect value are reported as deficient and escalated through a workflow. The workflow requires a follow-up action of the system owner, which is then recorded in SAP Process Control.

Key benefits
By shifting the monitoring to SAP Process Control, the cost of control decreases while the organization is better ensured that its controls operate effectively. By automating the parameter monitoring, the focus shifted to exceptions and follow-up. In the new situation, all results are also better auditable and thus useful for internal and external auditors.

9.2 Case 2: from Excel and manual consolidation to Process Control and integrated reporting

Context
A large multinational, active in over 100 countries, has its 2nd line performs a yearly test of design and test of effectiveness. These tests are executed by the local 2nd line teams in each country, the results are reviewed by the central 2nd line team. At the end of the testing cycle, all results need to be consolidated to prepare reports on the control effectiveness.

Situation prior to using SAP Process Control
Before SAP Process Control was used, the test of design and test of effectiveness were performed by populating ever growing Excel files. During the testing cycles, there was limited or no visibility on the testing status, the overall completion or effectiveness. Furthermore, the Excel files were shared across teams and no ownership could be appointed other than that of the team manager.

After the testing was completed, all results needed to be manually consolidated (also in Excel) in order to be able to use all data for reporting. This was performed by the central 2nd line team and usually took approximately 3 weeks.

Situation after
By using assessments in SAP Process Control, the questionnaires used for testing are now workflow-based. All controls now have a tester and reviewer assigned, which ensures ownership. After the tests have been scheduled, at any point in time the 2nd line teams can view the status of the tests, the overall completion rate and monitor the overall effectiveness.

On top of the standard system reports available, additional reports were created in Microsoft PowerBI. The reports are based on tables from SAP Process Control and consolidate all results from the testing cycles into dashboards, which are used for reporting. Consequently, the time needed for preparing the reports reduced from 3 weeks to 1 day.

Key benefits
SAP Process Control provided standardization and ownership of the testing processes. Reporting and consolidating were simplified and the administrative effort has decreased significantly.

9.3 Key lessons learned from various implementation projects

While SAP Process Control can provide substantial value, it is not always embraced by end-users, as it may limit flexibility and in some cases might invoke additional work. Change management and end-user engagement are therefore key aspects of every SAP Process Control implementation. In the long term, any system will only achieve success if the people working with it embrace and drive it. Furthermore, it is critical to engage the right 2nd / 3rd line and other relevant staff in the implementation project. Even though a

system implementation is sometimes approached as an IT project, in the case of SAP Process Control, it is a key success factor to also include the business (1st line), which will work with the system as well.

10 Conclusion

In this article, we have emphasized the importance of making the right choices when implementing SAP Process Control. For the master data, it is critical to focus on establishing the right organizational structure and integrating multiple control frameworks. For workflows, it is very important to determine the use cases and really integrate the organization's way of working into the system capabilities. For reporting, it is all about requirements and determining the right reports for the right audience. Finally, for control automation, it needs to be emphasized that SAP Process Control is not another data analytics tool, but a controls monitoring tool. Therefore, the focus should be on configuration settings. By considering the cautions and applying our suggestions, which are included in the online version of this article, SAP Process Control can be a useful solution to help organizations achieve their compliance goals.

11 References

Acknowledgement
This article is based on, and an expanded version of the article “A practical view on SAP Process Control, Getting in control step-by-step” in Compact Magazine, issue 2017/3, https://www.compact.nl/articles/a-practical-view-on-sap-process-control/

Lamberiks, G.J.L., Wouterse, S and De Wit, I. (2017), Trending topics in GRC tools, Compact 2017/3 (https://www.compact.nl/articles/trending-topics-in-grc-tooling/)

Assurance op marktwaardeberekeningen bij woningcorporaties

Elise Lassooij
Jesper de Boer

Elise is a Manager from the Risk Advisory team of Deloitte Netherlands. With 4.5 years of Third Party Assurance and IT auditing experience, she has performed many IT audits, ISAE3402/3000 assignments, and Advisory assignments in several industries. Elise holds a Master's degree in Business Information Management and an Executive Master's degree in IT Audit Compliance & Advisory.

Jesper de Boer is an IT-auditor and advisor at Deloitte. He started his career as a financial auditor but became more and more interested in IT-audit. So he switched in 2015 his focus and developed technical skills. His focus is performing large integrated audits at insurance companies, third party assurance and advisory. He is specialized in IT-maturity levels based on frameworks Cobit. He is also familiar with cyber frameworks like NIST, CIS and ISF.

1 Inleiding

1.1 Aanleiding

In de 20e eeuw waardeerden woningcorporaties hun vastgoed in de jaarrekening op historische kostprijs verminderd met afschrijvingen. Zij administreerden de waardering op papieren activa-kaarten, waarbij de jaarlijkse afschrijving met de pen werd bijgeschreven.
Sinds de verzelfstandiging van woningcorporaties begin jaren '90 was er meer behoefte aan inzicht in waardering van het vastgoed. Daarom werd in 1993 aan de hand van het Besluit beheer sociale-huursector (BBSH) de bedrijfswaarde ingevoerd. De bedrijfswaarde is de contante waarde van toekomstige inkomsten minus toekomstige uitgaven over de resterende levensduur van het bezit.
De bedrijfswaarde van een beperkt aantal woningen kan relatief eenvoudig worden berekend in een spreadsheet programma. Software leveranciers ontwikkelden applicaties om deze berekening voor grote aantallen woningen uit te voeren. Gebruikers en accountants controleerden de juistheid hiervan met gebruikmaking van eigen (deel-)berekeningen in spreadsheets.
De bedrijfswaarde wordt ook wel beleidswaarde genoemd. Een nieuw beleid, zoals een toekomstige huurverhoging of bezuiniging op onderhoud, leidt tot een andere bedrijfswaarde. Het toekomstige beleid zegt echter niets over de marktwaarde.
Om financiering van woningcorporaties mogelijk te maken, is financiële sturing nodig (Spelbos & Vlak, 2008). Daarvoor wenden de woningcorporaties zich tot banken. Commerciële banken kunnen echter de risico's louter op basis van de bedrijfswaarde niet goed inschatten. Zij zijn daarom meer geïnteresseerd in de marktwaarde. Voorheen hadden de staatsbanken "N.V. Bank Nederlandse Gemeenten" (BNG) en de "Nederlandse Waterschapsbank N.V." een groot aandeel in de financiering. Maar woningcorporaties willen en moeten, door de introductie van Basel III, steeds meer financiering aantrekken bij andere banken. Om deze reden ontstond ook bij de corporaties behoefte aan duidelijkheid over de marktwaarde.
Ook vanuit de politiek kwam druk om de marktwaarde inzichtelijk te maken. In de EU-beschikking "Steunmaatregelen nr. E 2/2005 en N 642/2009 – Nederland Bestaande steun en bijzondere projectsteun voor woningcorporaties" wordt staatssteun aan commerciële activiteiten verboden. Daarom heeft de Nederlandse overheid een splitsing in commerciële en sociale activiteiten verplicht gesteld via de Woningwet, artikel 45 (Woningwet, 2015). De commerciële activiteiten van woningcorporaties moeten administratief dan wel juridisch gescheiden zijn van sociale activiteiten. De bedrijfswaarde is niet geschikt om commerciële activiteiten te waarderen, de marktwaarde is hiervoor wel geschikt (Blok, 2013).
In de Woningwet 2015, artikel 35 lid 2, is opgenomen dat woningcorporaties het vastgoed dienen te waarderen op actuele waarde. Hieronder wordt verstaan de marktwaarde overeenkomstig het marktwaarde-begrip "onderhandse verkoopwaarde in verhuurde staat".
Het Besluit toegelaten instellingen volkshuisvesting (BTIV) 2015 heeft dit begrip nader uitgewerkt in artikel 31. Uit dit artikel blijkt dat woningcorporaties de marktwaarde op basis van de contante waarde van inkomende en uitgaande kasstromen moeten berekenen. De zogenaamde Discounted Cash Flow (DCF)-methode. Deze vorm van berekenen komt overeen met de manier van het berekenen van de bedrijfswaarde, echter moeten voor de marktwaardeberekening marktgegevens gebruikt worden.
Het waarderingshandboek "Handboek modelmatig waarderen marktwaarde 2016" (Minister voor Wonen en Rijksdienst, 2016) ondersteunt corporaties in het proces om tot waardering op marktwaarde te komen. Daarnaast is het bedoeld om de transparantie en onderlinge vergelijkbaarheid te vergroten. In het waarderingshandboek wordt onder andere aangegeven hoe de markthuur moet worden bepaald, hoe om te gaan met mutatiekans en wat de leegwaarde-ratio per regio is.

In figuur 1 staan de besluiten om te waarderen op marktwaarde aangegeven.

Het berekenen van de marktwaarde is veel complexer dan het berekenen van de bedrijfswaarde.

Figuur 1: Besluiten om op marktwaarde te waarderen

Een van de verschillen tussen bedrijfswaarde- en marktwaardeberekening betreft de disconteringsvoet. De bedrijfswaardeberekening kent maar één disconteringsvoet. De marktwaardeberekening kent een dis-conteringsvoet die afhankelijk is van een aantal factoren zoals risicovrije rentevoet, de vastgoed specifieke opslagen en de opslag voor het object- en marktrisico. Een ander verschil is dat bij de bedrijfswaarde-berekening de huurprijs een gegeven is, namelijk de prijs die de huurder op dit moment betaalt. Bij de markt-waardeberekening moeten de huurprijzen worden berekend.
Om uniformiteit bij woningcorporaties te bevorderen is modelmatig waarderen nodig. Dit is niet eenvoudig. Om foutieve berekeningen te voorkomen, zijn er keuzemogelijkheden (Merchant, 1982):

- Automatiseren van de gegevensverwerking.
- Centraliseren van besluitvorming (bijvoorbeeld het vierogenprincipe waarbij de manager altijd goedkeuring moet geven).
- Risicodeling met een derde partij (bijvoorbeeld een verzekeringsmaatschappij).
- Uitbesteden van de activiteiten aan een derde partij (bijvoorbeeld bij het ontbreken van de middelen om de complexe berekening zelf uit te voeren).

De woningcorporaties hebben gekozen voor automatiseren en hebben software aangeschaft die de markt-waardeberekening uitvoert. Het automatiseren van taken voorkomt een deel van eventuele menselijke fouten. De consistentie is groter dan in het geval de taken door mensen worden uitgevoerd. Softwareontwikkelaars spelen hierop in met als doel het eenvoudig en betrouwbaar berekenen van de marktwaarde. Op dit moment zijn er negen applicaties waarmee dit mogelijk is. De softwareontwikkelaars hebben de applicaties laten voorzien van assurance rapportages. Onafhankelijke auditors geven deze COS 3000 of NOREA 3000 assurance rapportages af. De opbouw van de rapportages en de gebruikte normenkaders zijn echter niet hetzelfde voor alle softwarepakketten.
Het bovenstaande maakt het interessant om te onderzoeken wat de toegevoegde waarde is van de assurance rapportages voor de berekening van de marktwaarde.

1.2 Onderzoeksdoelstelling en vraag

Het doel van ons onderzoek is om een concrete bijdrage te leveren aan toekomstige assurance rapportages voor marktwaardeberekening software. Enerzijds willen wij dit doen door inzichtelijk te maken wat de toegevoegde waarde is van de huidige assurance rapportages voor marktwaardeberekening software. Anderzijds willen wij een concrete bijdrage leveren in de vorm van een uniform normenkader dat alle IT-auditors in de toekomst kunnen gebruiken in de assurance rapportages.

Om deze onderzoeksdoelstelling te realiseren, beantwoorden wij in deze scriptie de volgende centrale vraagstelling:
Wat is de toegevoegde waarde van de assurance rapportages op de marktwaardeberekening software zoals die door woningcorporaties in Nederland wordt gebruikt?
Om deze vraagstelling te beantwoorden, zullen wij de volgende deelvragen onderzoeken:

- Waarom worden assurance rapportages verstrekt voor de software die marktwaardeberekeningen uitvoert voor woningcorporaties?
- Wat schrijven de COS 3000 richtlijnen en de NOREA 3000 richtlijnen voor, wat betreft assurance voor systeemonderzoeken?
- Welk normenkader achten wij noodzakelijk om assurance te kunnen geven op basis van de hierboven genoemde richtlijnen?
- Wat zien wij in de praktijk aan normenkaders terugkomen in de assurance rapportages en in hoeverre komen deze normenkaders overeen met ons voorgestelde normenkader?

Op basis van de NOREA 3000 richtlijnen en theorie betreffende de transactieverwerkingscyclus hebben wij een voorstel gemaakt voor een normenkader dat gebruikt kan worden voor systeemonderzoeken betreffende marktwaardeberekening software. Dit algemene normenkader hebben wij vervolgens vergeleken met de in praktijk gebruikte normenkaders voor systeemonderzoeken bij marktwaardeberekening softwarepakketten van woningcorporaties. De populatie van ons onderzoek betreft de assurance rapportages van alle marktwaarde-berekening softwarepakketten van woningcorporaties in Nederland. Dit zijn in totaal negen assurance rapportages voor negen software pakketten, van zeven leveranciers. Wij hebben de gehele populatie getest, waardoor wij geen steekproef technieken hoeven toe te passen of te verantwoorden.

2 Normenkader

2.1 Waarom worden assurance rapportages verstrekt?voor de software die marktwaardeberekeningen uitvoert voor woningcorporaties?

Wij behandelen deze vraag vanuit het oogpunt van de belangrijkste stakeholders van de marktwaarde, namelijk de softwareontwikkelaar, de woningcorporaties, de accountant en het Ministerie van Binnenlandse Zaken (BZK) en Koninkrijksrelaties.

Wij behandelen alle vier de zienswijzen omdat er sprake is van een sterke samenhang tussen deze partijen. Immers, het Ministerie van BZK houdt toezicht op de woningbouwsector (artikel 60 en 61 Woningwet) en stelt de accountantscontrole voor woningcorporaties verplicht (artikel 37 Woningwet).

2.1.1 De softwareontwikkelaar

In de wet zijn er in beginsel geen verplichtingen voor softwareontwikkelaars opgenomen. Dit betekent dat een softwareontwikkelaar een applicatie kan ontwikkelen, zonder dat deze aan eisen hoeft te voldoen.

De softwareontwikkelaar levert een product, namelijk de applicatie, en zal proberen deze te verkopen. Of de woningcorporaties dit software product in eigen beheer voeren of als SaaS-applicatie afnemen maakt in deze zin niet uit. De levering zal plaats vinden door middel van een licentie-overeenkomst. De woningcorporatie kan de softwareontwikkelaar aansprakelijk stellen indien de applicatie niet aan de eisen voldoet. Dit is geregeld in Afdeling 3, titel 3 van boek 6 van het Burgerlijk Wetboek. Zo kan de softwareontwikkelaar aansprakelijk worden gesteld op grond van het redelijkerwijs te verwachten gebruik van het product. Maar volgens dit wetboek is de softwareontwikkelaar niet verplicht om software van een assurance rapport te laten voorzien.

2.1.2 De woningcorporaties

Uit wet- en regelgeving blijkt niet dat woningcorporaties verplicht zijn om marktwaardeberekening software te laten voorzien van assurance. In de praktijk komt de vraag van woningcorporaties voor assurance voort uit de druk die de accountant oplegt voor de controle van de jaarrekening.

2.1.3 De accountant

Zoals aangegeven in de inleiding, zijn berekeningen door de komst van de marktwaarde complexer geworden. De berekeningen van marktwaardes kunnen niet eenvoudig door een schaduwberekening gecontroleerd worden. De marktwaarde is een belangrijk onderdeel van de jaarrekening. Dit blijkt bijvoorbeeld uit de jaarrekening van de grootste (in eenheden) corporatie van Nederland, Ymere (Jaarverslag Ymere, 2016). Het balanstotaal bedraagt € 10,9 miljard, waarvan € 10,6 miljard gebaseerd is op de marktwaarde van het vastgoed. De berekening is dus een significant onderdeel van de jaarrekening.

De accountant dient in de planningsfase van de jaarrekeningcontrole een risicoanalyse uit te voeren. Daarbij maakt de accountant onderscheid in normale en significante risico's (COS 315.27). Aan significante risico's moet de accountant meer aandacht besteden dan aan normale risico's. Voorbeelden hiervan zijn de extra aandacht voor interne beheersing (COS 330.15) en het uitvoeren van meer detailcontroles (COS 330.30). Aanwijzingen voor een significant risico zijn opgenomen in COS 315.28:

1 De vraag of het risico verband houdt met recente significante ontwikkelingen op economisch, boekhoudkundig of ander gebied en daarom specifieke aandacht vereist.
2 De complexiteit van transacties.
3 De mate van subjectiviteit bij het waarderen van financiële informatie met betrekking tot het risico, vooral als de waardering veel onzekerheid inhoudt.

Figuur 2: Marktwaarde in jaarrekeningcontrole

Deze aanwijzingen zien we terug bij het beoordelen van de marktwaarde, omdat de marktwaardeberekening afhankelijk is van economische parameters en van interpretatie van wet- en regelgeving. Ook is de marktwaardeberekening complex. De accountant zal daarom de juistheid van de marktwaarde als een significant risico identificeren.

Een andere taak van de accountant in de planning van zijn controle is om na te gaan of de woningcorporatie de marktwaarde met een applicatie berekent. De controlerichtlijn (COS 315.A62) zegt over het gebruik van informatietechnologie voor de interne beheersing: “Over het algemeen komt informatietechnologie de interne beheersing van een entiteit ten goede omdat ze de entiteit in staat stelt vooraf bepaalde bedrijfsregels consistent toe te passen en complexe berekeningen uit te voeren bij het verwerken van grote hoeveelheden transacties of gegevens.”

De accountant kan de berekening gebruiken als controleinformatie. Hieraan zijn wel voorwaarden verbonden (COS 500.9): “Wanneer de accountant gebruik maakt van informatie die afkomstig is van de entiteit, dient hij te evalueren of die informatie voldoende betrouwbaar is voor de doeleinden van de accountant, en dient hij naargelang nodig in de gegeven omstandigheden:

1 controle-informatie te verkrijgen over de nauwkeurigheid en volledigheid van de informatie; en
2 te evalueren of de informatie voldoende nauwkeurig en gedetailleerd is voor de doeleinden van de accountant.
3 elementen te selecteren die moeten worden getoetst om controle-informatie te verkrijgen.”

De controlestandaarden geven hiermee het belang aan, dat de accountant moet vaststellen dat de be-rekening van de woningcorporatie betrouwbaar is. Het gebruikmaken van een assurance rapport voor software die in beheer is van de woningcorporatie, is niet specifiek in de controlestandaarden genoemd. Indien de applicatie is uitbesteed aan een service-organisatie, bieden de controlestandaarden de optie om gebruik te maken van een assurance rapportage. Dit is geen verplichting. De accountant kan namelijk ook zelf naar de service-organisatie toegaan of een opdracht geven aan een andere auditor (COS 402.16 letters b en c). De accountant kan de assurance rapportage gebruiken voor inzicht in de service-organisatie (COS 402.1 t/m 12) of steunen op de beheersingsmaatregelen van de service-organisatie (COS 402.17).

2.1.4 Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De accountant voert naast zijn jaarrekeningcontrole ook andere assurance werkzaamheden uit specifiek voor de toezichthouder, zijnde de Autoriteit woningcorporaties. Dit is geregeld in artikel 36a lid 4 en artikel 37 van de Woningwet. In deze artikelen staat dat de Minister door middel van ministeriële regelingen voorschriften kan geven. Deze voorschriften zijn het Besluit toegelaten instellingen volkshuisvesting en het accountantsprotocol 2016 (Minister voor Wonen en Rijksdienst, 2015). De Minister voor Wonen en Rijksdienst was destijds belast met een aantal beleidsterreinen van het Ministerie van BZK. In het accountantsprotocol 2016 is het volgende opgenomen:

“De accountant stelt vast of bij het rekenmodel dat door de toegelaten instelling is gehanteerd bij het berekenen van de marktwaarde voor de dVi, een assurance rapportage is afgegeven conform COS 3000/3402.”

Op grond van deze regelgeving is de accountant verplicht om vast te stellen of er een assurance rapportage aanwezig is. Tevens stelt de accountant vast of de woningcorporatie eventuele bevindingen uit de assurance rapportage juist en volledig aan de Autoriteit woningcorporaties meldt.

Uit bovenstaande inventarisatie blijkt dat een assurance rapport verwacht wordt op basis van het accoun-tantsprotocol, dat door de Minister voor Wonen en Rijksdienst is vastgesteld. In de volgende paragraaf analyseren wij welke richtlijnen er zijn voor de assurance rapportage.

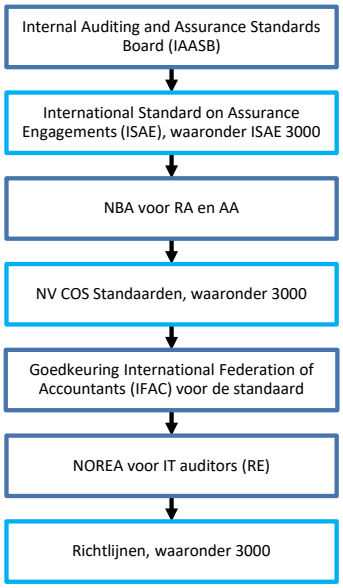
Omdat richtlijnen recent zijn gewijzigd, gaan wij na welke partijen hierbij betrokken zijn. Wij willen weten hoe de richtlijnen tot stand komen (2.2.1). Daarna analyseren wij welke richtlijnen (3000 of 3402) het meest geschikt zijn voor de assurance rapportage (2.2.2).

2.2 Richtlijnen betreffende assurance voor systeemonderzoeken

2.2.1 Hoe komen richtlijnen tot stand?

De Internal Auditing and Assurance Standards Board (IAASB) maakt standaarden voor auditors en publiceert deze standaarden in het “Handbook of Internal Quality Control, Auditing, Review, Other Assurance, and Related Services”, dat periodiek verschijnt. De laatste versie dateert uit 2016/2017. De Nederlandse Beroeps-organisatie van Accountants (NBA) neemt deze standaarden veelal ongewijzigd of met een beperkt aantal aanpassingen over in de “Nadere voorschriften controle- en overige standaarden (NV COS)”. De vertaling vanuit het Engels gebeurt met inachtneming van de “Policy Statement-Policy for Translating and Reproducing Standards” van de International Federation of Accountants (IFAC). De IFAC ondersteunt de IAASB bij het uitvoeren van deze processen. De IFAC stelt vast of eventuele aan-passingen ten opzichte van de standaard van IAASB aanvaardbaar zijn.

De orde van NOREA beslist of er nieuwe of aangepaste richtlijnen komen (art. 4 van de statuten). Het bestuur van NOREA dient deze richtlijnen aan te dragen bij de orde van NOREA. Het bestuur van NOREA neemt veelal standaarden over van het NBA (NV COS). Het bestuur laat zich hierbij ondersteunen door commissies, waaronder de Commissie Beroepsregels (art. 20 van de statuten). Deze commissie voert consultaties uit bij de leden om praktijkervaring te vernemen. Op grond daarvan neemt de ledenvergadering van de orde het besluit om richtlijnen aan te passen dan wel te introduceren. De NOREA heeft in bijlage 1 van het “Stramien voor Assuranceopdrachten” de structuur van gedrags- en beroepsregels weergegeven. In deze structuur zijn de richtlijnen voor assurance opdrachten opgenomen. NOREA onderscheidt twee richtlijnen voor assurance opdrachten, de richtlijnen 3000 en de richtlijn 3402.



Figuur 3: Samenhang IAASB – NBA - NOREA

2.2.2 Welke richtlijnen (3000 of 3402) zijn het meest geschikt?

Omdat we in deze scriptie rapportages analyseren met een Nederlandse doelgroep van IT-auditors met een RE titel, hanteren wij de NOREA richtlijnen. Als voorbeeld van een assurance opdracht noemt NOREA systeemonderzoeken (artikel 39 van “Stramien voor Assuranceopdrachten”). De assurance opdrachten van NOREA zijn op te delen in: "Assurance opdrachten" (richtlijnen 3000) en "Assurance rapporten interne beheersing serviceorganisatie" (richtlijn 3402). Richtlijn 3402 is een specifieke invulling van de algemene richtlijn 3000. Richtlijn 3402 is bedoeld voor de audit van service-organisaties in het kader van de jaarrekeningcontrole. Bij de software applicaties voor marktwaarde is niet altijd sprake van een service-organisatie. Daarom is richtlijn 3000 het beste geschikt voor ons onderzoek.

2.3 Een uniform normenkader om assurance te geven op basis van de hierboven genoemde richtlijn

Een NOREA 3000 assurance rapportage moet voldoen aan de vereisten in de richtlijn. Het normenkader hiervoor hebben wij beschreven in de volgende paragraaf (2.3.1). Daarnaast is het belangrijk dat uit de rapportage blijkt, welke normen door de IT-auditor zijn getoetst. Die normen betreffen de kwaliteit van de software. Deze komen in de assurance rapportages tot uitdrukking in de tekst van de verklaring, maar zijn veelal als bijlage bijgevoegd. Ook voor dit onderdeel hebben wij aan de hand van theorie een normenkader ontwikkeld dat in paragraaf 2.3.2 is uitgewerkt.

2.3.1 NOREA normenkader

Om tot een normenkader te komen, hebben wij alle artikelen en toelichtende teksten uit de NOREA 3000 richtlijn doorgenomen. In het normenkader hebben wij verplichtingen, die moeten blijken uit de rapportage, opgenomen. Vereisten die niet uit de rapportage blijken, zoals het tijdig

plannen van de opdracht, hebben wij niet meegenomen in het normenkader. Het tijdig plannen van de opdracht, blijkt immers niet uit de rapportage.

De richtlijnen voor de attest- en directe-opdracht verschillen op onderdelen. Artikelen die overeenkomen, hebben wij éénmalig opgenomen. Voor artikelen die niet overeenkomen, hebben wij een splitsing aangebracht in het normenkader voor NOREA 3000A of NOREA 3000D.

In het normenkader hebben wij de integrale tekst uit het artikel vertaald naar een voor ons onderzoek toetsbare norm.

2.3.2 Software normenkader

Waar de NOREA richtlijn 3000 ingaat op de processen omtrent het opstellen van het rapport en de rol van de IT-auditor, is de kwaliteit van de assurance rapportage tevens afhankelijk van het normenkader dat is gebruikt om de software te toetsen. In deze paragraaf gaan wij in op welk normenkader wij noodzakelijk achten om assurance te kunnen geven over de marktwaardeberekening software. Hierbij is het belangrijk om te begrijpen dat de marktwaardeberekening software uitsluitend rekent en geen verhuur- of vastgoed-administratie bevat.

Een IT-auditor kan assurance op software geven op basis van verschillende normen en controles, afhankelijk van verschillende invalshoeken. Hij kan assurance geven op processen die hebben geleid tot het software product, maar ook op het software product zelf. Wij onderscheiden drie typen normen die gebruikt kunnen worden bij het geven van assurance op software: ontwikkelnormen, beheernormen en softwarenormen.

Allereerst kan een IT-auditor assurance geven over het ontwikkelproces. De controles die door de software leverancier zijn gehanteerd ten tijde van het ontwikkelen van de software hebben invloed op projectuitkomsten zoals tijd en geld en de kwaliteit van het eindproduct. In paragraaf 2.3.2.1 gaan wij dieper in op de toegevoegde waarde van software ontwikkelnormen in het kader van de assurance die gegeven wordt op de marktwaardeberekening software die gebruikt wordt door woningcorporaties.

Wanneer het ontwikkelproces afgerond is en de software in gebruik is, wordt de software beheerd. Dit beheerproces omvat onder andere logische toegangsbeveiliging, wijzigingsbeheer en back-upbeheer. Beheerprocessen, en dan voornamelijk logische toegangsbeveiliging en wijzigingsbeheer, hebben invloed op de juistheid en volledigheid van de data in het systeem. De beheernormen en controles lichten wij toe in paragraaf 2.3.2.2.

Daarnaast kan er gekeken worden naar de functionering van de software, zoals de gebruikte broncode en inrichting van applicatiecontroles. De focus ligt hier op product assurance. De software in scope van de assurance rapportages betreft software die marktwaarde van verhuureenheden berekent. Deze berekeningen dienen de rekenregels, zoals opgenomen in het “Handboek modelmatig waarderen marktwaarde”, te volgen. De software normen betreffende de kwaliteit van de software en de ingerichte berekeningen zijn hier van belang. In paragraaf 2.3.2.3 behandelen wij softwarenormen.

Ontwikkelnormen

Bij het ontwikkelen van de software heeft de broncode grote invloed op de productkwaliteit van het systeem. De broncode van een systeem beïnvloedt direct vijf kwaliteitsattributen: functionele geschiktheid, prestatie-efficiëntie, betrouwbaarheid, beveiligbaarheid en onderhoudbaarheid (Amoraal et al., 2013). Daarmee heeft het softwareontwikkelproces tevens invloed op het inherente risico

van latere audits die het systeem in scope hebben. Het inherente risico, het interne controle risico en het ontdekkingsrisico geven samen het accountantscontrolerisico aan. Voor definities zie tabel 1 (Van der Perk & Kromhout, 2007).

Risico	Definitie
Accountantscontrole risico	Het risico dat de accountant, ondanks zorgvuldige uitvoering van zijn controleprogramma, onbewust een onjuiste verklaring afgeeft bij een verantwoording die onvolkomenheden van materieel belang bevat.
Inherente risico	Het risico dat materiële onjuistheden in de verantwoording optreden, afgezien van het effect van bestaande interne beheersingssystemen.
Interne controle risico	Het risico dat materiële onjuistheden niet of niet tijdig door de interne beheersingsmaatregelen worden voorkomen, dan wel niet of niet tijdig worden gesignaleerd en gecorrigeerd.
Ontdekkingsrisico	Het risico dat materiële onjuistheden noch door de interne beheersing noch door de accountant worden gesignaleerd en gecorrigeerd.

Tabel 1: Audit risico's.
Bron: Van der Perk & Kromhout (2007)

Hoewel het software ontwikkelproces invloed heeft op het inherente risico van latere financiële audits die het systeem in scope hebben, achten wij de risico's van het softwareontwikkelproces niet relevant voor de assurance rapportages voor de marktwaardeberekening software. Om vast te stellen of de software goed rekent, kijkt de IT-auditor direct naar de code die is ingericht voor het uitvoeren van de berekeningen. Een eventuele verkeerde inrichting van de berekeningscode als gevolg van het ontwikkelproces, zal de IT-auditor dus tijdens zijn onderzoek achterhalen. Het beheer van de berekeningscode van de gebruikte applicatie zou wel relevant kunnen zijn, omdat wijzigingen in de berekeningscode invloed hebben op het resultaat van de marktwaardeberekeningen. In de volgende paragraaf gaan wij verder in op de beheernormen die relevant zijn voor de assurance rapportages.

Beheernormen
Ervan uitgaande dat de berekeningscode conform het waarderingshandboek is ingericht tijdens de ontwikkel-fase, kan de accountant enige mate van zekerheid verkrijgen over dat de marktwaardeberekeningen juist en volledig zijn uitgevoerd gedurende een bepaalde periode. Dit is mogelijk als de juiste beheernormen zijn ingericht in de organisaties die met de marktwaardeberekening software te maken hebben, te weten de software leveranciers en de woningcorporaties. Van alle ITIL beheerprocessen zijn wijzigingsbeheer (inclusief scheiding ontwikkel- en productieomgeving) en logische toegangsbeveiliging, relevante beheerprocessen voor de assurance rapportages. De reden is dat deze beheerprocessen invloed hebben op de juistheid en de volledigheid van de rekenregels in het systeem (Van der Perk & Kromhout, 2007).

Wijzigingsbeheer
Het Ministerie BZK actualiseert het waarderingshandboek jaarlijks. Een aanpassing in het handboek kan bijvoorbeeld een aanpassing in de macro-economische parameters zijn (zoals indexeringen). De softwareontwikkelaar vertaalt het handboek in de berekeningscode. Of de software leverancier deze aanpassingen door middel van iteraties in de agile-aanpak of via de traditionele software ontwikkeling maakt, doet er in dit geval niet toe. De woningcorporaties zijn immers alleen geïnteresseerd in de laatste versie van de software, die alle wijzigingen van het handboek bevat. Hiermee

berekent de woningcorporatie jaarlijks éénmalig de marktwaarde ten behoeve van de jaarrekening. Daarom is ook de accountant uitsluitend geïnteresseerd in de laatste versie van de software, die ten grondslag ligt aan de marktwaarde die in de jaarrekening van de woningcorporatie is opgenomen.

Als wij het wijzigingsbeheer in de context van de woningcorporaties en hun marktwaardeberekening software plaatsen, is wijzigingsbeheer door de jaarlijkse actualisatie van het handboek niet relevant voor de financieel accountant. Hierdoor is product assurance over het marktwaarde-berekening software product dat de accountant in scope heeft ten tijde van de jaarrekeningcontrole voldoende. De financieel accountant wil daarom controleren of het software product dat de woningcorporatie gebruikt voor zijn jaarrekening, gelijk is aan het software product waar assurance over is gegeven in een NOREA 3000 rapport. Artikel 69d van de NOREA richtlijnen schrijft voor dat “de rapportage dient een beschrijving van het niveau van zekerheid te bevatten en een beschrijving van het onderzoeksobject”. Op basis van dit artikel hebben wij een norm in ons normenkader opgenomen die waarborgt dat de assurance rapportage een beschrijving van het onderzoeksobject, zoals de naam en het versienummer van het software product, bevat.

In theorie zouden ongeautoriseerde wijzigingen in de berekeningscode gemaakt kunnen worden, zonder dat het versienummer van de applicatie wordt verhoogd. Echter, de software leverancier heeft als derde partij geen baat bij het foutief aanpassen van de rekenregels. Een medewerker of het management van de woningcorporatie zou dit wel kunnen hebben. De enige beheersingsmaatregel die relevant is, met betrekking tot wijzigingsbeheer, is daarom dat de eindgebruiker (de woningcorporatie) geen mogelijkheid heeft tot het aanpassen van de rekenregels. Deze beheersingsmaatregel hebben wij in het normenkader opgenomen, zie tabel 3.

Logische toegangsbeveiliging
Hoewel de accountant alleen ten tijde van de jaar-rekeningcontrole hoeft te weten of de marktwaardeberekening juist en volledig is, wil de accountant wel vaststellen of de gegevens die gebruikt worden bij de berekening (bijvoorbeeld gegevens m.b.t. de verhuureenheden) betrouwbaar zijn. Enerzijds kunnen deze gegevens ingevoerd of aangepast worden door de eindgebruiker (woningcorporaties), anderzijds zou de leverancier gegevens kunnen wijzigen door middel van de directe toegang tot database tabellen die de ingevoerde gegevens bewaren voor de berekening. Ook hier geldt dat de software leverancier als derde partij geen baat heeft bij het foutief aanpassen van de gegevens in de tabellen. Wat overblijft, is logische toegangsbeveiliging aan de eindgebruikerskant (woningcorporaties), om te waarborgen dat alleen geautoriseerde medewerkers gegevens met betrekking tot de woningen kunnen invoeren. Beheersingsmaatregelen met betrekking tot logische toegangsbeveiliging dienen getest te worden door de accountant van de woningcorporaties. Deze beheersingsmaatregelen zullen dus als gebruikersoverwegingen opgenomen worden in de assurance rapportages.

Wanneer de accountant van de woningcorporatie de logische toegangsbeveiliging met betrekking tot de invoer van gegevens wil toetsen, is het belangrijk om te begrijpen dat de marktwaardeberekening software uitsluitend rekent en geen verhuur- of vastgoedadministratie bevat. De woningcorporaties beschikken over een aparte applicatie voor de verhuur- en vastgoedadministratie. In de praktijk heeft de verhuur- of vastgoedadministratie applicatie soms niet alle mogelijkheden om die gegevens op te slaan die nodig zijn voor de marktwaardeberekening. Het kan daarom zijn dat de woningcorporatie een data verrijkingsslag maakt bij het importeren van de gegevens in de marktwaardeberekening software.

Software normen

In paragraaf 2.3.2.2 over beheernormen nemen wij aan dat de berekeningscode conform het waarderings-handboek is ingericht. Maar hoe weten we of de software werkt zoals hij zou moeten werken? Om de relevante software normen voor een systeembeoordeling (product assurance) te bepalen, is het allereerst belangrijk om een strategische analyse uit te voeren en om inzicht te verwerven in het geautomatiseerde systeem. Wanneer de strategische analyse voldoende inzicht geeft in de reden voor het onderzoek en het object van het onderzoek is bepaald, kunnen de risico's gedefinieerd worden (Boer, 2017). Aan de hand van deze risico's kunnen de relevante software normen bepaald worden.

In paragraaf 2.1 zijn wij dieper ingegaan op de vraag "Waarom worden er assurance rapportages verstrekt voor de software die marktwaardeberekeningen uitvoert voor woningcorporaties", waarmee wij inzicht hebben gekregen in de achterliggende redenen voor het assurance onderzoek en tevens inzicht hebben gekregen in het object van het onderzoek namelijk de software die marktwaardeberekeningen uitvoert. Om nu de risico's te bepalen, dienen we te begrijpen wat de software precies doet. De marktwaardeberekening software dient als operationele ondersteuning en verwerkt input van gegevens van de verhuureenheden zoals de beheerkosten, huurstijgingspercentages en de disconteringsvoet. Na de input vindt de transactieverwerking en rapportage plaats. Dit alles tesamen is de transactieverwerkingscyclus. De transactieverwerkingscyclus bestaat volgens Van Praat (2014) uit vijf onderdelen. Deze vijf onderdelen hebben wij hieronder opgesomd en gerelateerd aan de marktwaardeberekening software:

- Het invoeren van gegevens
  - Invoeren van de verhuureenheden.
  - Invoeren van parameters die nodig zijn om de marktwaarde te bepalen, zoals de beheerkosten, huurstijging percentages en de disconteringsvoet.
- De transactieverwerking zelf
  - Gebruik van rekenregels conform het waarderingshandboek.
  - Gebruik van tabellen die de ingevoerde gegevens opslaan alvorens deze worden aangewend voor de marktwaardeberekening.
- Het onderhouden van de bestanden
  - Opslaan van de uitkomsten van de berekeningen.
- Het genereren van rapporten
  - Genereren van (management) rapporten die de marktwaarde weergeven.
- Het verwerken van informatieaanvragen
  - Opvragen van de marktwaarde van één of meer specifieke verhuureenheden.

Aan elke hierboven genoemde processtap van de transactieverwerkingscyclus voor de marktwaardebe-rekening zijn één of meer risico's verbonden. De risico's zijn benoemd in tabel 2 en zijn specifiek gemaakt voor de marktwaardeberekening software. Voor vier van de vijf processtappen is per processtap één risico gedefinieerd. Bij de tweede processtap, de transactieverwerking, zijn drie risico's gedefinieerd waarbij wij zijn uitgegaan van geprogrammeerde rekenregels die een beroep doen op tabellen die gegevens bevatten voor de marktwaardeberekeningen. De invoer van gegevens uit de eerste processtap leidt tot aanpassing van deze tabellen. Maar het kan voor komen dat ongeautoriseerde wijzigingen rechtstreeks worden gemaakt in de tabellen, waarmee de eerste processtap, invoer van gegevens, wordt overgeslagen.

Transactieverwerkingcyclus	Risico
1. Invoer van gegevens	Onjuiste data met betrekking tot de woningen worden ingevoerd of ingelezen.
2. Transactieverwerking	Ongeautoriseerde wijzigingen worden gemaakt in de tabellen die gegevens bevatten voor de marktwaardeberekeningen.
	De marktwaardeberekening wordt niet conform het waarderingshandboek uitgevoerd.
	Ongeautoriseerde wijzigingen worden gemaakt in de rekenregels voor de marktwaardeberekeningen.
3. Onderhoud van de bestanden	Uitkomsten (marktwaarden) kunnen na de berekeningen nog aangepast worden.
4. Rapporten genereren	Rapporten die de marktwaarden weergeven zijn niet juist en/of volledig.
5. Informatieaanvragen verwerken	Het onjuist weergeven van de marktwaarde van specifieke verhuureenheden.

Tabel 2: Risico's van de transactieverwerkingscyclus

Om de risico's te mitigeren, hebben wij beheersingsdoelstellingen en bijbehorende beheersingsmaatregelen opgesteld, zie tabel 3. Bij het opstellen van deze beheersingsdoelstellingen en beheersingsmaatregelen is geredeneerd vanuit de transactieverwerkingscyclus voor de marktwaardeberekening.

Voor het eerste risico "onjuiste data met betrekking tot de woningen worden ingevoerd of ingelezen", hebben wij bij de beheersingsmaatregelen geprogrammeerde controles voor de invoervelden opgenomen. In theorie zou de woningcorporatie de invoer van gegevens ook manueel kunnen controleren. De IT-auditor heeft echter het doel om software product assurance te geven. De marktwaardeberekeningen zijn zodanig afhankelijk van de kwaliteit van de ingevoerde data, dat de software leverancier geprogrammeerde controles in dient te richten om het software product van toegevoegde waarde te laten zijn. Het waarderingshandboek "Handboek modelmatig waarderen marktwaarde 2016" (Minister voor Wonen en Rijksdienst, 2016) heeft alle parameters gespecificeerd die nodig zijn voor de marktwaardeberekening. Wij hebben dit handboek geanalyseerd en per parameter gekeken welke geprogrammeerde controle ingericht moet zijn in de applicatie, zie hiervoor Appendix A. Hoewel Van Praat (2014) uitgaat van vijf typen geprogrammeerde controles, achten wij de typen totaalcontrole en verbandcontrole niet relevant als invoercontrole, omdat de ingevoerde gegevens slechts objectgegevens betreffen, die geen relatie hebben tot andere gegevens. Wij zijn daarom uitgegaan van de drie overige typen geprogrammeerde controles:

1 Bestaanbaarheidscontroles
2 Redelijkheidscontroles
3 Volledigheidscontroles

In de laatste kolom van het normenkader voor de marktwaardeberekening software (tabel 3) hebben wij aangegeven welke beheersingsmaatregelen getest moeten worden in de product assurance rapportages, conform onze beredenering in paragraaf 2.3.2.2 en 2.3.2.3. We zien in tabel 3 dat beheersingsmaatregel 1, 2, 5, 8 en 11 t/m 13 in scope zijn voor de marktwaardeberekening software assurance rapportages.

Object	Transactie-verwerking-cyclus	Risico	Beheersingsdoel-stelling	#	Beheersingsmaatregel	In scope van marktwaardebe-rekening software assurance rapport?
Marktwaar-deberekening applicatie	1. Invoer van gegevens	Onjuiste data met betrekking tot de wo-ningen worden in-gevoerd of ingelezen	De software leve-rancier heeft be-heersings-maatre-gelen getroffen om met een rede-lijke mate van ze-kerheid te waar-borgen dat de data met betrek-king tot de wonin-gen juist en volle-dig wordt inge-voerd	1	Geprogrammeerde controles zijn ingericht voor de invoervelden (zie Appendix A)	Ja, dit is een application con-trol
				2	Een audittrail is inge-richt waaruit blijkt wie welke data wanneer heeft ingevoerd	Ja, dit is een application con-trol
				3	Alleen geautoriseerde medewerkers kunnen gegevens m.b.t. de woningen invoeren	Nee, gebruikersoverweging die getoetst wordt door de ac-countant van de woningcorpo-ratie
	2. Transactie-verwerking	Ongepaste wijzigingen worden ge-maakt in de tabellen die gegevens bevatten voor de marktwaar-debereke-ningen		4	Alleen geautoriseerde medewerkers kunnen tabellen die gegevens bevatten voor de marktwaardebereke-ningen beheren	Nee, deze beheersingsmaatre-gel hoeft niet aan de kant van de software leverancier getest te worden, omdat de software leverancier geen baat heeft bij het foutief aanpassen van de gegevens, refereer naar para-graaf 2.3.2.2
	2. Transactie-verwerking	De markt-waardebe-rekening wordt niet conform het waar-derings-handboek uitgevoerd	De software leve-rancier heeft be-heersings-maatre-gelen getroffen om met een rede-lijke mate van ze-kerheid te waar-borgen dat de re-kenregels de marktwaardebe-rekening conform het waarderings-handboek uitvoe-ren	5	Rekenregels van het handboek zijn juist en volledig ingericht in het systeem	Ja, dit is een application con-trol
	2. Transactie-verwerking	Ongepaste wijzigingen worden ge-maakt in de rekenregels voor de marktwaar-debereke-ningen		6	Wijzigingen in de re-kenregels worden be-heersd (conform een wijzigingsbeheerpro-ces) doorgevoerd	Nee, wijzigingsbeheer is niet van toepassing, refereer naar paragraaf 2.3.2.2
				7	Alleen geautoriseerde medewerkers kunnen rekenregels in de pro-ductieomgeving aan-passen	Nee, deze beheersingsmaatre-gel hoeft niet aan de kant van de software leverancier getest te worden, omdat de software leverancier geen baat heeft bij het foutief aanpassen van de rekenregels, refereer naar pa-ragraaf 2.3.2.2
				8	De eindgebruiker (wo-ningcorporatie) kan geen rekenregels in de productieomgeving aanpassen	Ja, refereer naar paragraaf 2.3.2.2
				9	Wijzigingen in de re-kenregels worden ge-test alvorens de wijzi-gingen worden door-gevoerd in de produc-tieomgeving	Nee, wijzigingsbeheer is niet van toepassing, refereer naar paragraaf 2.3.2.2
				10	Wijzigingen worden akkoord bevonden door de productei-genaar alvorens de wijzi-gingen worden door-gevoerd in de produc-tieomgeving	Nee, wijzigingsbeheer is niet van toepassing, refereer naar paragraaf 2.3.2.2

	3. Onderhoud van de bestanden	Uitkomsten (marktwaarden) kunnen na de berekeningen nog aangepast worden	De software leverancier heeft beheersings-maatregelen getroffen om met een redelijke mate van zekerheid te waarborgen dat de applicatie de marktwaarden juist, volledig weergeeft	11	Uitkomsten (marktwaarden) kunnen na de berekeningen niet meer aangepast worden	Ja, dit is een application control
	4. Rapporten genereren	Rapporten die de marktwaarden weergeven zijn niet juist en/of volledig		12	Rapporten moeten de volgende identificatiegegevens laten zien: - Datum en tijdstip van het rapport - Titel van het rapport - Paginanummering	Ja, dit is een application control
				13	Rapporten moeten de selectiecriteria laten zien.	Ja, dit is een application control
				14	Rapporten moeten de volgende totaalgegevens laten zien: - Totaal van ingevoerde verhuureenheden - Totale marktwaarde van alle verhuureenheden	Nee, deze beheersingsmaatregel dient slechts voor de gebruikers-vriendelijkheid van het rapport en is daarom geen vereiste
	5. Informatie-aan-vragen verwerken	Het onjuist weergeven van de marktwaarde van specifieke verhuureenheden		15	De applicatie geeft bij het opvragen van marktwaarden de datum weer van de invoer van de gegevens die tot de marktwaardeberekening hebben geleid	Nee, deze beheersingsmaatregel is n.v.t. omdat alleen de rapporten worden gebruikt door de accountant

Tabel 3: Normenkader marktwaardeberekening software

3 Discussie

Het doel van dit onderzoek is om de toegevoegde waarde te bepalen van de assurance rapportages op de marktwaardeberekening software zoals die door woningcorporaties in Nederland wordt gebruikt. Deze sectie reflecteert op de resultaten van ons onderzoek en bespreekt de praktische implicaties.

3.1 Waarom worden assurance rapportages verstrekt?

Bijna alle gevraagde partijen geven aan dat de assurance rapportages een vereiste zijn vanuit de accountant en het accountantsprotocol. Echter, komt de vraag voor bewijs van een betrouwbare marktwaarde uiteindelijk vanuit het Ministerie van BZK. Wat opvalt, is dat het Ministerie van BZK de software assurance voor de marktwaardeberekening software niet verplicht stelt en zelf onderzoeksbureaus heeft ingeschakeld om het waarderingshandboek en de marktwaardeberekeningen te valideren. Uit het waarderingshandboek validatie onderzoek van Onderzoeksbureau Abf blijkt dat de systematiek voor rekenmodellen niet volledig vastligt. Uit het onderzoek van Onderzoeksbureau Fakton blijkt dat de uitkomsten van de marktwaarden afwijken. Aangezien alle IT-auditors een goedkeurende verklaring af hebben gegeven, kunnen we vraagtekens zetten bij de toegevoegde waarde van de assurance rapportages. Wij stellen dat er drie redenen zijn die het geven van assurance op de marktwaardeberekening software bemoeilijken.

Allereerst is het waarderingshandboek op meerdere manieren te interpreteren. Zolang het waarderings-handboek niet tot één interpretatie leidt, kunnen de auditors eigenlijk hun onderzoek niet uitvoeren. Immers controleren is toetsen aan een norm, waarbij de norm eenduidig en begrijpelijk moet zijn (NOREA, 2016). Het Ministerie van BZK moet het waarderingshandboek aanscherpen en/of testdata beschikbaar stellen. De testdataset kan bestaan uit input van verschillende typen objecten (woningen, bedrijfsonroerendgoed, zorgvastgoed, parkeerplaatsen, etc), met meerdere scenario's en de uitkomsten op basis van het handboek.

Ten tweede, de IT-auditors hanteren uiteenlopende methoden om de inrichting van de rekenregels te valideren. Hoewel alle IT-auditors uiteindelijk een goedkeurende verklaring hebben afgegeven, kunnen de grote verschillen uit het onderzoek van Onderzoeksbureau Fakton niet alleen het gevolg zijn van een paar onduidelijkheden in het waarderingshandboek. De IT-auditors zullen zich moeten afvragen of zij op de juiste manier de rekenregels hebben getoetst.

Ten derde, het Ministerie van BZK publiceert het waarderingshandboek erg laat. Het handboek 2016 is op 16 november 2016 gepubliceerd. Dat komt mede doordat bepaalde macro-economische parameters op peildatum (31 december) van andere instanties, zoals Centraal Planbureau, laat beschikbaar komen. Hierna dienen softwareontwikkelaars de aanpassingen in hun marktwaarde-applicaties te verwerken. Woningcorporaties moeten daarna de software testen en de input verzorgen, waarna de accountant voor 1 juli 2017 de verklaring bij de jaarrekening dient af te geven.

Op grond van onze analyse concluderen wij dat:

1 Uit validatie van het handboek blijkt dat de rekenregels op meerdere manieren te interpreteren zijn (bevinding W1)
2 Een testdataset ontbreekt (bevinding W2)
3 De rekenregels zijn niet juist getoetst (bevinding W3)
4 Tussen publicatie van het handboek en de deadline voor het gebruik van de marktwaardeberekening software zit een beperkte tijd (bevinding W4)

3.2 NOREA richtlijnen

Zolang de assurance rapportages wel verstrekt worden conform COS 3000/3402, moet de IT-auditor zich aan de NOREA richtlijnen houden. Het is goed dat de NOREA richtlijnen overeenkomen met de NBA richtlijnen en dat zij gebaseerd zijn op één internationale standaard. De richtlijnen bevatten hiervoor een goed raamwerk met onderdelen als opdrachtaanvaarding, planning, uitvoering en rapportage. Echter de richtlijnen bevatten naar onze mening onvoldoende aanknopingspunten om tot uniforme assurance rapportages te komen. Dit blijkt uit de door ons onderzochte assurance rapportages. De paragrafen in deze assurance rapportages verschillen qua naamgeving, inhoud en volgorde. Dat bemoeilijkt de onderlinge vergelijkbaarheid en heeft een negatieve invloed op de kwaliteit. Naar onze mening is een voorbeeld rapportage noodzakelijk. In andere richtlijnen, zoals NOREA richtlijn 3402, is wel een voorbeeld assurance rapportage opgenomen.

Kijkend naar de bevindingen, vallen ons drie zaken op. Ten eerste verwijst geen enkele assurance rapportage expliciet naar de per 1 januari 2017 nieuwe NOREA richtlijnen. Wij vragen ons af of de IT-auditors zich wel voldoende bewust waren van deze nieuwe richtlijnen.

Ook opvallend is dat één assurance rapportage op acht vereisten afwijkt van de richtlijnen. Inhoudelijk ontbreekt een normenkader met criteria en goede gebruikersoverwegingen. Deze rapportage voldoet naar onze mening niet aan de vereisten van een goede assurance rapportage. Zowel de woningcorporatie als hun accountant zullen extra werkzaamheden moeten uitvoeren om de betrouwbaarheid van de marktwaardeberekening aan te tonen. Hoewel drie assurance rapportages op enkele onderdelen ook niet aan de nieuwe richtlijnen voldoen, hoeven de woningcorporaties en hun accountants naar onze mening slechts beperkte extra werkzaamheden uitvoeren voordat zij de assurance rapportage kunnen gebruiken voor hun controle werkzaamheden.

Als laatste valt op dat slechts uit drie assurance rapportages blijkt dat een vastgoeddeskundige is ingeschakeld. Gezien de afwijkingen in berekende marktwaarden tussen de software pakketten, zoals vastgesteld door Onderzoeksbureau Fakton, is het naar onze mening wel noodzakelijk dat de IT-auditors vastgoeddeskundigen inzetten. De vastgoeddeskundigen zouden ingezet moeten worden voor de risico-analyse. Het handboek bevat veel rekenregels, die soms complex te interpreteren zijn. Er zijn rekenregels die een grote impact hebben op de marktwaarde en regels die een beperkte invloed hebben. Een IT-auditor kan willekeurig rekenregels toetsen. Maar om de rekenregels te toetsen die er toe doen, is het naar onze mening verstandig om gebruik te maken van een vastgoeddeskundige.

Op grond van onze analyse concluderen wij dat:

1 De NOREA 3000 richtlijnen bevatten onvoldoende aanknopingspunten om tot uniforme assurance rapportages te komen. Een voorbeeld NOREA 3000 assurance rapportage ontbreekt (bevinding N1)
2 De nieuwe NOREA 3000 richtlijnen lijken niet bij een ieder bekend (bevinding N2)
3 Één van de negen assurance rapportages is niet bruikbaar voor de accountant van de woningcorporatie (bevinding N3)
4 De inzet van vastgoeddeskundigen is beperkt. Vastgoeddeskundigen zouden ingezet moeten worden voor de risico-analyse (bevinding N4)

3.3 Software normen

Bij het opstellen van het software normenkader zijn wij uitgegaan van de transactieverwerkingscyclus. Uit de geanalyseerde rapportages blijkt dat slechts in één van de negen rapportages alle software normen zijn opgenomen die wij hebben gedefinieerd in hoofdstuk 2, tabel 3. Alle overige IT-

auditors lijken niet de volledige transactieverwerkingscyclus te hebben overwogen bij het opstellen van het normenkader. In zes rapportages zijn zelfs uitsluitend de rekenregels getoetst.

Wat ook opvalt, is dat in drie rapportages software normen zijn opgenomen die betrekking hebben op versiebeheer en wijzigingsbeheer. Wij hebben in hoofdstuk 2 (paragraaf 2.3.2.2) beargumenteerd waarom deze normen niet getoetst hoeven te worden. Er zijn dus werkzaamheden uitgevoerd die niet uitgevoerd hoefden te worden om tot een oordeel te komen.

De rekenregels zijn op verschillende manieren getoetst. De grote verschillen in uitkomsten van marktwaardeberekeningen tussen de verschillende software pakketten kunnen niet alleen het gevolg zijn van een paar onduidelijkheden in het waarderingshandboek. De IT-auditors zullen zich moeten afvragen of zij op de juiste manier de rekenregels hebben getoetst.

In één rapport is geen normenkader opgenomen. Aan de beschrijving van de werkzaamheden is af te leiden dat de rekenregels zijn getoetst. Het is niet af te leiden of de overige, door ons gedefinieerde, beheersingsmaatregelen zijn getoetst.

Op grond van onze analyse concluderen wij dat:
1 In acht van de negen rapportages lijkt de IT-auditor niet de volledige transactieverwerkingscyclus te hebben overwogen bij het opstellen van het normenkader (bevinding S1)
2 In drie rapportages zijn normen opgenomen die de IT-auditor naar onze mening niet hoeft te toetsen (bevinding S2)
3 De rekenregels zijn niet juist getoetst. Refereer naar bevinding W3.
4 Een van de negen assurance rapportages is niet bruikbaar voor onze analyse (bevinding S3)

4 Conclusie

Ter afronding van de scriptie komen wij in dit hoofdstuk tot de conclusies op de deelvragen en de centrale vraag.

Deelvraag: Waarom worden assurance rapportages verstrekt voor de software die marktwaardeberekeningen uitvoert voor woningcorporaties?

De assurance rapportages worden verstrekt omdat de accountants van de woningcorporaties en de Autoriteit woningcorporaties (Aw) hierom vragen.
Uit ons onderzoek blijkt dat de software leveranciers, de branchevereniging en één woningcorporatie wijzen naar de accountants van de woningcorporaties. Immers de accountants willen zekerheid bij de door de woningcorporaties berekende marktwaarde. De woningcorporaties vinden het zelf belangrijk, maar ook weer niet zo belangrijk dat zij actief de assurance rapportages analyseren.
De accountants en de Inspectie Leefomgeving en Transport (waar de Autoriteit woningcorporaties onder valt) wijzen naar het accountantsprotocol. In het accountantsprotocol is opgenomen dat een assurance rapportage op de marktwaardeberekening software moet worden afgegeven conform COS 3000/3402. De Aw, die uiteindelijk valt onder politieke verantwoordelijkheid van het Ministerie van BZK, geeft aan het belangrijk te vinden dat woningcorporaties betrouwbare marktwaarden berekenen. Ook het Ministerie van BZK wil een consistente berekening van marktwaarden zien bij de woningcorporaties, omdat zij het maatschappelijk bestemd vermogen (MBV, afgeleid van de marktwaarde) van woningcorporaties willen vergelijken. Het Ministerie van BZK zelf geeft aan dat er geen verplichting is om de marktwaardeberekening software te laten voorzien van assurance rapportages.

Deelvraag: Wat schrijven de COS 3000 richtlijnen en de NOREA 3000 richtlijnen voor, wat betreft assurance voor systeemonderzoeken?

Uit het literatuuronderzoek in paragraaf 2.2 blijkt dat, met ingang van 1 januari 2017, de richtlijnen zijn herzien. De nieuwe richtlijnen zijn uitgebreider. In de nieuwe richtlijnen is nadrukkelijker aangegeven, wat in de assurance rapportage moet staan. Daarnaast is zowel een attest als directe opdracht mogelijk. Specifieke richtlijnen voor systeemonderzoeken zijn niet opgenomen, de richtlijnen zijn algemeen geformuleerd.

Deelvraag: Welk normenkader achten wij noodzakelijk om assurance te kunnen geven op basis van de hiervoor genoemde richtlijnen?

In paragraaf 2.3 hebben wij een normenkader ontwikkeld. Het normenkader is opgedeeld in twee delen. Het eerste deel betreft een normenkader op basis van de inhoudelijke teksten van de NOREA richtlijnen. De richtlijnen hebben wij integraal beoordeeld op vereisten die in de assurance rapportages moeten terug komen.
Het tweede deel betreft de software normen die door de IT-auditor moeten worden getoetst. Deze normen, die betrekking hebben op de kwaliteit van de software, geven product assurance. Ook voor dit onderdeel hebben wij aan de hand van theorie een normenkader ontwikkeld. Wij onderscheiden drie typen normen die gebruikt kunnen worden bij het geven van assurance op software: ontwikkelnormen, beheernormen en softwarenormen. Wij hebben onderzocht of ontwikkelnormen relevant zijn voor de audit van de marktwaardeberekening software. Dat blijkt niet het geval, omdat de IT-auditor uitsluitend wil vaststellen wat de huidige inrichting van de rekenregels is.
De beheernormen, waaronder wijzigingsbeheer en logische toegangsbeveiliging zijn beperkt relevant. Uit ons onderzoek blijkt dat de eindgebruiker geen wijzigingen mag doorvoeren en dat de eindgebruiker zelf verantwoordelijk is voor de logische toegangsbeveiliging. Dit zijn normen die wij in het normenkader hebben opgenomen.
De software normen, op basis van de transactieverwerkingscyclus, blijken het meest relevant. De transactieverwerking begint bij de invoer van gegevens. Aan de hand van het handboek hebben wij invoercontroles geformuleerd. Ook voor de andere onderdelen van de transactieverwerking hebben wij relevante normen bepaald.

Deelvraag: Wat zien wij in de praktijk aan normenkaders terugkomen in de assurance rapportages en in hoeverre komen deze normenkaders overeen met ons voorgestelde normenkader?

Wij hebben de negen assurance rapportages van alle marktwaardeberekening software pakketten in Nederland vergeleken met ons voorgestelde NOREA en software normenkader. Alle assurance rapportages zijn afgegeven volgens de 3000D richtlijn, met een redelijke mate van zekerheid en bevatten een goedkeurend oordeel.
Geen enkele assurance rapportage voldoet aan alle NOREA normen. Geen van de rapportages verwijst expliciet naar de per 1 januari 2017 nieuwe NOREA richtlijnen of geeft expliciet aan dat richtlijn 3000D (directe-opdrachten) of 3000A (assertion opdrachten) is gevolgd. Eén assurance rapportage wijkt zelfs op acht vereisten af van de richtlijnen. Deze rapportage voldoet naar onze mening niet aan de vereisten van een goede assurance rapportage. Zowel de woningcorporatie als hun accountant zullen extra werkzaamheden moeten uitvoeren om de betrouwbaarheid van de marktwaardeberekening aan te tonen. Hoewel drie assurance rapportages op enkele onderdelen ook niet aan de nieuwe richtlijnen voldoen, hoeven de woningcorporaties en hun accountants naar onze mening slechts beperkte extra werkzaamheden uit te voeren voordat zij de assurance rapportage kunnen gebruiken voor hun controle werkzaamheden. Wat verder opvalt, is dat slechts uit drie assurance rapportages blijkt dat een vastgoeddeskundige is ingeschakeld. Gezien de afwijkin-

gen in berekende marktwaarden tussen de software pakketten, zoals vastgesteld door Onderzoeksbureau Fakton, is het naar onze mening wel noodzakelijk dat de IT-auditors vastgoeddeskundigen inzetten. De vastgoeddeskundigen zouden ingezet moeten worden voor de risico-analyse.
Uit de analyse op software normen in de rapportages blijkt dat slechts in één van de negen rapportages alle software normen zijn opgenomen die wij hebben gedefinieerd in hoofdstuk 2. Alle overige IT-auditors lijken niet de volledige transactieverwerkingscyclus te hebben overwogen bij het opstellen van het normenkader. In zes rapportages zijn zelfs alleen de rekenregels getoetst. Wat ook opvalt, is dat in drie rapportages software normen zijn opgenomen die betrekking hebben op beheerprocessen. Wij hebben in hoofdstuk 2 beargumenteerd waarom deze normen niet getoetst hoeven te worden. Er zijn dus werkzaamheden uitgevoerd die niet uitgevoerd hoefden te worden om tot een oordeel te komen. Één van de negen assurance rapportages bleek niet bruikbaar voor onze analyse, omdat de IT-auditor geen normenkader heeft opgenomen in de rapportage.

Centrale vraag: Wat is de toegevoegde waarde van de assurance rapportages op de marktwaardeberekening software zoals die door woningcorporaties in Nederland wordt gebruikt?

Duidelijk is dat de assurance rapportages nog verbeterd kunnen worden. Enerzijds omdat zij niet aan de huidige NOREA richtlijnen voldoen. Anderzijds omdat de getoetste software normen nog niet voldoen aan het software normen die wij hebben bepaald op basis van theorie. De opzet en inhoud van de assurance rapportages verschillen, wat een vergelijking tussen de rapportages bemoeilijkt.

Het Ministerie van BZK heeft onderzoeksbureaus ingeschakeld om het waarderingshandboek en de marktwaardeberekeningen te valideren. Uit het waarderingshandboek validatie onderzoek van Onderzoeksbureau Abf blijkt dat de systematiek voor rekenmodellen niet volledig vastligt. Uit het onderzoek van Onderzoeksbureau Fakton blijkt dat de uitkomsten van de marktwaarden, zoals berekend door de negen pakketten, afwijken. Aangezien alle IT-auditors een goedkeurende verklaring af hebben gegeven, kunnen we vraagtekens zetten bij de toegevoegde waarde van de assurance rapportages.

Onze conclusie is derhalve dat de toegevoegde waarde op dit moment beperkt is. De toegevoegde waarde kan worden vergroot door een uniform normenkader. In Appendix A hebben wij een voorbeeld assurance rapport uitgewerkt, dat aan het NOREA normenkader voldoet en waarin ons software normenkader is opgenomen. Het Ministerie van BZK zou de publicatie van het handboek kunnen vervroegen en een testdataset met berekeningsuitkomsten beschikbaar kunnen stellen. De IT-auditors zijn nog niet klaar wanneer zij ons NOREA en software normenkader toepassen. Zij zullen tevens moeten overwegen of zij op de juiste manier de rekenregels toetsen.

5 Aanbevelingen en beperkingen

Naar aanleiding van de bevindingen, zijn in dit hoofdstuk onze aanbevelingen en beperkingen opgenomen.

Aanbevelingen
Allereerst raden wij aan om een voorbeeld assurance rapportage met een vaste indeling en inhoud op te stellen, ten behoeve van de vergelijking tussen de rapportages (bevinding N1). Wij stellen voor om de NOREA 3000D richtlijn aan te houden, omdat deze richtlijn toepasbaar is voor de IT-auditor en omdat alle normen uit het door ons opgestelde software normenkader direct te testen zijn. Aangezien er geen normen zijn opgenomen die betrekking hebben op de beheersomgeving

van de leverancier, is een attest rapport niet nodig. Voor de NOREA 3000D kan gedacht worden aan de volgende inhoudsopgave:

Inhoudsopgave:	Wat dient dit te omvatten:
Assurance rapport van de onafhankelijke auditor	Deze titel is verplicht (artikel 69 letter a).
Opdracht en reikwijdte	De reikwijdte gaat in op de opdrachtomschrijving, zoals redelijke of beperkte mate van zekerheid, een verwijzing naar het normenkader en het object van onderzoek (marktwaarde-applicatie).
Verantwoordelijkheden van softwareontwikkelaar	Hierin moet staan wat de verantwoordelijkheden van het management van de softwareontwikkelaar zijn, waaronder de opzet en bestaan van beheersingsmaatregelen rondom de marktwaarde-applicatie.
Verantwoordelijkheden auditor	Uit deze paragraaf moet blijken dat richtlijnen 3000D zijn gevolgd en dat de IT-auditor van mening is dat hij voldoende en geschikte controle-informatie heeft als onderbouwing van het oordeel. Daarnaast moeten verwijzingen naar het Reglement Gedragscode ('Code of Ethics') en het Reglement Kwaliteitsbeheersing NOREA (RKBN) of soortgelijke stelsels zijn opgenomen.
Beperkingen	Hieruit blijken voorbehouden, bijvoorbeeld dat de audit is gericht op een brede groep van woningcorporaties. Op individueel niveau kunnen namelijk andere aspecten van belang zijn. Daarnaast blijkt uit deze paragraaf dat de getoetste informatie over interne beheersingsmaatregelen niet alle fouten bij het berekenen van de marktwaarde kan voorkomen. Verder is de assurance rapportage afgegeven bij één bepaalde versie van de marktwaarde-applicatie, alle andere versies zijn niet getoetst.
Gebruikersoverwegingen	De woningcorporaties zijn verantwoordelijk voor de input van objectgegevens. Ook zijn zij verantwoordelijk voor het wijzigings- en autorisatiebeheer en maatregelen dat de data niet door onbevoegden wordt aangepast.
Beoogde gebruikers en doel	De beoogde gebruikers zijn woningcorporaties en hun accountant. Hierin staat dat de auditor de verspreidingskring beperkt tot woningcorporaties en hun accountants.

Tabel 4: Voorstel inhoudsopgave NOREA 3000D assurance rapport

Wij hebben geconstateerd dat IT-auditors de nieuwe richtlijnen nog niet expliciet toepassen (bevinding N2). Bovendien hebben wij geconstateerd dat niet alle assurance rapportages voldoen aan de normen in het NOREA normenkader (bevinding N3). Deze richtlijnen zijn verplicht per 1 januari 2017. De NOREA richtlijnen zijn vastgesteld in de ledenvergadering. Uit de notulen van de ledenvergadering (Algemene Vergadering NOREA, 2016) blijkt beperkt wat de wijzigingen zijn en welke gevolgen dit heeft voor de assurance rapportages. Op de ledenvergadering zijn niet alle leden aanwezig. Wij raden NOREA aan om bijvoorbeeld een artikel te publiceren op de website www.deitauditor.nl. Een alternatief is om een bijeenkomst te organiseren voor IT-auditors gericht op NOREA 3000.

De IT-auditors zetten beperkt vastgoeddeskundigen in, terwijl wij verwachten dat zij bij de risicoanalyse een vastgoeddeskundige inzetten (bevinding N4). Wij raden IT-auditors aan om hiervan wel gebruik te maken. Zij kunnen de rekenregels in het handboek op waarde inschatten en bepalen welke rekenregels echt relevant zijn. De IT-auditor voert steekproeven uit om vast te stellen dat de marktwaardeberekening software rekent conform het handboek. Door risico-gericht te selecteren kan de IT-auditor het aantal waarnemingen beperken en een efficiëntere en effectievere controle uitvoeren.

Voor het toetsen van de software dienen de IT-auditors de gehele transactieverwerkingscyclus te analyseren bij het opstellen van het software normenkader (bevinding S1). Zij kunnen het door ons gedefinieerde software normenkader toepassen. Uiteraard dient de IT-auditor dit software normenkader wel specifiek te maken voor het desbetreffende marktwaardeberekening software pakket. Wij raden de IT-auditors aan niet meer testen dan strikt noodzakelijk (bevinding S2). Wanneer het NOREA normenkader en het softwarenormenkader worden toegepast, zullen alle rapporten goed te vergelijken zijn voor de eindgebruiker (bevinding N3 en S3). Wat de IT-auditor bespaart op het budget, indien hij minder controles hoeft uit te voeren, kan hij aanwenden voor het beter testen van de rekenregels (bevinding W3).

Wij hebben in Appendix A een voorbeeld opgenomen van een NOREA 3000D assurance rapportage dat voldoet aan ons NOREA en software normenkader.

Uit validatie van het handboek blijkt dat de rekenregels op meerdere manieren te interpreteren zijn (bevinding W1). Softwareontwikkelaars moeten aannames doen. Wij begrijpen dat het opstellen van een waarderingsmodel niet eenvoudig is. Maar het mag naar onze mening niet zo zijn dat de rekenregels op meerdere manieren te interpreteren zijn, waardoor de uitkomst anders is. Wij raden daarom het Ministerie van BZK aan om regels en definities in het handboek eenduidig en simplistisch op te stellen. Ook raden wij aan om een standaard testdatasest met daarin objectgegevens en de verwachte marktwaarden beschikbaar te stellen (bevinding W2). Door de uitkomsten van deze testdataset te vergelijken met de verwachtte uitkomsten, kan de volledigheid van de rekenregels worden vastgesteld. De verbetering van het handboek en de testdataset bieden de IT-auditors de mogelijkheid om de rekenregels beter te controleren (bevinding W3). Immers, wanneer er verschillen naar voren komen bij het doorvoeren van de testdataset, heeft de IT-auditor aanleiding om het onderzoek (de steekproef van rekenregels) uit te breiden.

Tussen publicatie van het handboek en de deadline voor het gebruik van de marktwaarde-applicaties zit een beperkte tijd (bevinding W4). Dat komt mede doordat bepaalde macro-economische parameters op peildatum (31 december) pas laat van andere instanties, zoals Centraal Planbureau, beschikbaar komen. Naar onze mening is dat geen reden om te wachten met publiceren van het handboek. Immers de methodiek van waarderen staat dan al lang vast. En juist deze methodiek kost de softwareontwikkelaars de meeste tijd om te programmeren. Wij raden het Ministerie van BZK aan om het handboek eerder te publiceren en zelfs voor meer boekjaren vast te stellen. De macro-economische parameters kunnen later door middel van een update worden gepubliceerd.

Beperkingen

In ons onderzoek zijn wij uitgegaan van één moment van berekening van de marktwaarde bij één bepaalde versie van de marktwaardeberekening software. Dat is namelijk het geval voor de berekening van de marktwaarde op peildatum 31 december in verband met het opstellen van de jaarrekening. Ons onderzoek is niet bruikbaar indien gebruikers zekerheid willen over meerdere versies van de marktwaardeberekening software of over meerdere berekeningen in een periode. Dit kan het geval zijn indien woningcorporaties of andere type bedrijven de marktwaardeberekening software gebruiken voor vastgoedsturing of investeringen.

Een tweede en derde beperking betreffen de invoer van objectgegevens. De invoercontroles zijn opgesteld op basis van het waarderingshandboek van 2016. Bij een volgend waarderingshandboek zal de IT-auditor moeten bepalen of de invoercontroles aangepast moeten worden. Wij veronderstellen dat gebruikers de gehele invoer verrichten in de versie die is voorzien van een assurance rapportage. Ons onderzoek is derhalve niet geschikt indien gebruikers in een eerdere versie de invoer verrichten.

6 Referenties

ABF Research (2016). Validatie Handboek modelmatig waarderen marktwaarde. Referentieunmmer r2016-0056MK.

Amoraal, J., Lanzani, G., Kuiters, P. en Koedijk J. (2013). Grip op de kwaliteit van software. Compact, 2013/2.

Blok, S.A. (2013, 6 september). Viertal toezeggingen inzake woningcorporaties [Kamerbrief]. Geraadpleegd van https://zoek.officielebekendmakingen.nl/kst-29453-329.html

Boer, H. (2017, 31 maart). 2.4. Compliance & Auditing "Systeemonderzoeken & BPA" [college slides 19-59]. Geraadpleegd van https://bb.vu.nl/webapps/blackboard/content/listContent.jsp?course_id=_114979_1&content_id=_2570990_1&mode=reset

Bryman, A., & Bell, E. (2007). Business Research Methods (2nd ed.). Oxford.

Capers Jones, T. (1994). Assessment and Control of Software Risks. University of California: Yourdon Press.

Choudhury, V. en Sabherwal, R, (2003). Portfolios of Control in Outsourced Software Development Projects. Information Systems Research 14, nr 3: 291-314.

Dyba, T. en Dingsøyr, T. (2008). Empirical studies of agile software development: A systematic review. Inform. Softw. Technol. 50: 833-859

Eisenhardt, K.M. (1989). Building Theories from Case Study Research. Academy of Management Review, 14: 532-50.

Europese Commissie (z.j.). EU beschikking “Steunmaatregelen nr. E 2/2005 en N 642/2009 – Nederland Bestaande steun en bijzondere projectsteun voor woningcorporaties. Geraadpleegd van http://docplayer.nl/17281712-Steunmaatregelen-nr-e-2-2005-en-n-642-2009-nederland-bestaande-steun-en-bijzondere-projectsteun-voor-woningcorporaties.html

Hattink, C. J. (2016). Being in control with agile. Compact, 2016/1.
IFAC. (z.j.). Assurance Engagements Other than Audits or Reviews of Historical Financial Information. Geraadpleegd van https://www.iaasb.org/projects/assurance-engagements-other-audits-or-reviews-historical-financial-infor Rubin en Rubin (2011). Supporting agile software development through active documentation. Requirements Engineering 16, nr 2: 117-132.
IFAC. (z.j.). Clarity of IAASB Standards. Geraadpleegd van https://www.iaasb.org/projects/clarity-iaasb-standards

IFAC. (z.j.). Standaard 3000 (Herzien) Assurance opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie. Geraadpleegd van http://www.ifac.org/publications-resources/standaard-3000-herzien-assurance opdrachten-anders-dan-opdrachten-tot International Auditing and Assurance Standards Board (IAASB). (2016). Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements - 2016/2017 Edition, Volume II. doi: 978-1-60815-318-3

James, B. (2013). Notulen van meeting IAASB Consultative Advisory Group op 9-10 september 2013 in New York. Onderwerp: Assurance Engagements other than Audits or Reviews–ISAE 3000
Stichting Ymere (2016). Jaarverslag 2016 van Stichting Ymere

Kirsch, L. (1996). The management of complex tasks in organizations: Controlling the systems development process. Organizational Science 7, nr 1: 1-21.

Merchant, K. A. (1982). The Control Function of Management. Sloan Mangement Review, Summer, 43-55

Minister voor Wonen en Rijksdienst (2016). Regeling van de Minister voor Wonen en Rijksdienst van 29 november 2016, houdende enkele technische wijzigingen van de Regeling toegelaten instellingen volkshuisvesting 2015 en een indexering van geldbedragen in het Besluit toegelaten instellingen 2015 (nr. 2016-0000756632). Geraadpleegd van https://zoek.officielebekendmakingen.nl/stcrt-2016-67521.html

Minister voor Wonen en Rijksdienst (2015). Accountantsprotocol regeling Toegelaten instellingen volkshuisvesting 2015 (verslagjaar 2016), zoals opgenomen in bijlage 4 van Regeling van de Minister voor Wonen en Rijksdienst van 19 januari 2017 (nr. 2017-0000034415). Geraadpleegd van https://zoek.officielebekendmakingen.nl/stcrt-2017-4313.html?zoekcriteria=%3fzkt%3dEenvoudig%26pst%3d%26vrt%3dnr.%2b2017-0000034415%26zkd%3dInDeGeheleText%26dpr%3dAfgelopenDag%26sdt%3dDatumBrief%26ap%3d%26pnr%3d1%26rpp%3d10&resultIndex=2&sorttype=1&sortorder=4

NBA (2011). NBA brief aan IAASB. Onderwerp: "ED ISAE 3000", datum 1 september 2011, kenmerk: KvH

NBA (2017). NV COS 3000 richtlijnen. Geraadpleegd van https://www.nba.nl/tools/hra-2017/

Naik, B. (2009, maart). PROJECT PROPOSAL Revision of ISAE 3000. IAASB Main Agenda, pp. 1-22

NOREA. (z.j.). Consultatie herziening Raamwerk en Richtlijn 3000. Geraadpleegd van https://besloten.accountweb.nl/Norea/Actueel/Nieuws/Consultatie+herziening+Raamwerk+en+Richtlijn+3000.aspx

NOREA (2011). NOREA brief aan IAASB. Onderwerp: "ED ISAE 3000", datum 1 september 2011, kenmerk: Ab/wo

NOREA (2016). Artikel 44 van STRAMIEN VOOR ASSURANCE OPDRACHTEN van 14 december 2016

NOREA (2016). Notulen ledenvergadering van 14 december 2016

NOREA (2017). NOREA 3000 en 3402 richtlijnen. Geraadpleegd van https://www.norea.nl/regels-en-richtlijnen

Praat, J. van. (2014). Reader Processen in de organisatie. Amsterdam, Nederland: Vrije Universiteit Amsterdam

Spelbos, B. en Vlak, A. (2008). Woningcorporaties kampen met veranderingen in financiële sturing. Vastgoedmarkt/Woningen, mei 2008/23

Stake, R.E. (1995). The Art of Case Study Research (Thousand Oaks, Calif.: Sage)

Van der Perk, L. J. en Kromhout, P. N. M. (2007). Testen van applicatiecontroles. Compact 2007/3.

Woningwet, geldend van 1 juli 2017. Geraadpleegd van http://wetten.overheid.nl/BWBR0005181/2017-07-01/0/afdrukken

Appendix A
Voorbeeld assurance rapport

Assurance rapport van de onafhankelijke auditor van softwareontwikkelaar X over de beschrijving van interne beheersingsmaatregelen en hun opzet

Aan: softwareontwikkelaar X

Opdracht en reikwijdte
Wij hebben in opdracht van softwareontwikkelaar X een assurance opdracht uitgevoerd gericht op het verkrijgen van een redelijke mate van zekerheid of de beheersingsdoelstellingen, zoals geformuleerd in het in Bijlage A opgenomen normenkader voor de marktwaarde-applicatie Y met versie Z van softwareontwikkelaar X, in alle van materieel belang zijnde aspecten op [OnderzoeksDatum] zijn gerealiseerd met behulp van de in het normenkader genoemde beheersingsmaatregelen.

De marktwaarde-applicatie Y met versie Z berekent op basis van het Handboek modelmatig waarderen marktwaarde zoals opgenomen in “bijlage 2 van Regeling van de Minister voor Wonen en Rijksdienst van 29 november 2016 (nr. 2016-0000756632)” de marktwaarde. De marktwaarde-applicatie Y berekent de marktwaarde aan de hand van objectgegevens, macro-economische en model-parameters.

Verantwoordelijkheden van softwareontwikkelaar X
Softwareontwikkelaar X is verantwoordelijk voor het opzetten, implementeren en effectief laten werken van interne beheersingsmaatregelen om de vermelde interne beheersingsdoelstellingen te bereiken.

Verantwoordelijkheden van de auditor
Het is onze verantwoordelijkheid een assurance rapport te verstrekken inzake de vraag of de beheersingsdoelstellingen voor de marktwaarde-applicatie Y met versie Z zoals opgenomen in bijlage A met een redelijke mate van zekerheid in alle van materieel belang zijnde aspecten op [OnderzoeksDatum] zijn gerealiseerd met behulp van de in het normenkader genoemde beheersingsmaatregelen.

We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht, waaronder Richtlijn 3000D 'assurance opdrachten door IT-auditors' vastgesteld door Nederlandse Orde van Register EDP-auditors (NOREA). Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of, in alle van materieel belang zijnde aspecten, de interne beheersingsmaatregelen opgenomen in bijlage A op afdoende wijze zijn opgezet en bestaan om de beheersingsdoelstellingen genoemd in bijlage A te realiseren.

Wij zijn onafhankelijk van Softwareontwikkelaar X zoals vereist in Richtlijn 3000D (herzien) 'assurance opdrachten door IT-auditors' en het Reglement Gedragscode ('Code of Ethics'). Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) voor Assurance opdrachten toe die regels bevat voor het inrichten van een kwaliteitssysteem in een accountantseenheid. Op grond hiervan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van ethische voorschriften, accountantsstandaarden en standaarden voor IT-auditors en andere relevante wet- en regelgeving.

Ons onderzoek omvat mede die werkzaamheden die wij in de omstandigheden nodig achten om een toereikende zekerheid te verkrijgen voor het afgeven van ons oordeel, waaronder het testen of de beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen voor de marktwaarde-applicatie Y zoals opgenomen in bijlage A op afdoende wijze zijn opgezet ("opzet) en effectief zijn geïmplementeerd ("implementatie").

Zoals hierboven staat vermeld, hebben wij geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen die bij de beschrijving waren inbegrepen en brengen derhalve daarover geen oordeel tot uitdrukking.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel te bieden.

Criteria
Als toetsingscriteria hebben wij het in bijlage A opgenomen normenkader gehanteerd. Wij hebben dit normenkader op [datumafstemming] afgestemd met softwareontwikkelaar X.
Wij zijn van mening dat dit normenkader toereikend is voor het doel van de assurance opdracht.

Beperkingen van interne beheersingsmaatregelen bij de softwareontwikkelaar X
Het onderzoek is gericht op beheersingsmaatregelen ten behoeve van de beheersingsdoelstellingen voor de marktwaarde-applicatie Y, in opzet en bestaan. Onder "opzet en bestaan" verstaan wij het aantoonbaar vaststellen van de effectiviteit van de beheersingsmaatregel op het moment van onderzoek. Het testen van de effectieve werking van de beheersingsmaatregel voor of na de gehanteerde onderzoeksdatum ([OnderzoeksDatum]) heeft geen onderdeel uitgemaakt van ons onderzoek.
Buiten de reikwijdte van onze opdracht vielen verder onder meer:
- De juistheid, tijdigheid en volledigheid van de door cliënten in te voeren gegevens, waaronder de objectgegevens en parameters.
- Beheersingsmaatregelen aan de kant van de cliënten, waaronder het authentificatie-, autorisatie- en wijzigingsbeheer, maar ook toegang tot de database.
- Beheersingsdoelstellingen en beheersingsmaatregelen welke niet zijn opgenomen in het normenkader zoals opgenomen in bijlage A.
- Andere waarderingshandboeken dan over 2016. De risico-analyse is uitgevoerd op basis van waarderingshandboek 2016. Andere waarderingshandboeken vallen buiten de scope van deze opdracht.
- Andere versies dan versie Z van de marktwaarde-applicatie Y.

De audit is gericht op een brede groep van cliënten. Op individueel niveau kunnen andere aspecten van belang zijn.

Oordeel
Naar ons oordeel, in alle van materieel belang zijnde aspecten, zijn de interne beheersingsdoelstellingen voor de marktwaarde-applicatie Y zoals opgenomen in bijlage A, op [OnderzoeksDatum] met een redelijke mate van zekerheid gerealiseerd

Beoogde gebruikers en doel

Dit assurance rapport en bijlagen zijn één geheel, dat alleen als geheel ter beschikking mag wordn gesteld aan de doelgroep bestaande uit de (toekomstige) gebruikers van de marktwaarde-applicatie Y versie Z van softwareontwikkelaar X en hun accountants. De doelgroep dient voldoende inzicht te hebben om de risico's op afwijkingen van het materieel belang in de financiële overzichten in te schatten. Dit met inbegrip van informatie over interne beheersingsmaatregelen die door gebruikers zelf worden uitgevoerd. Verstrekking van het assurance rapport aan anderen is uitsluitend toegestaan nadat wij hiervoor onze schriftelijke toestemming hebben verleend.

[Handtekening van de auditor van de softwareontwikkelaar X]

[Datum van het assurance rapport van de auditor van de softwareontwikkelaar X]
[Het adres van de auditor van de softwareontwikkelaar X]

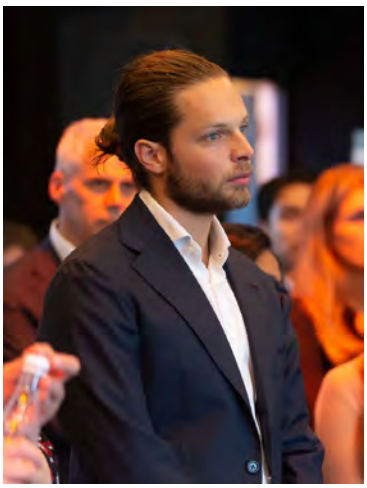
Bijlage A Normenkader - behorend bij Appendix D voorbeeld assurance rapport

Transactie-verwerkingcyclus	Beheersingsdoelstelling	#	Beheersingsmaatregel	Conclusie beheersingsmaatregel	Conclusie beheersingsdoelstelling
1. Invoer van gegevens	De software leverancier heeft beheersingsmaatregelen getroffen om met een redelijke mate van zekerheid te waarborgen dat de data met betrekking tot de woningen juist en volledig wordt ingevoerd	1	Geprogrammeerde controles zijn ingericht voor de invoervelden (zie Appendix A)		
		2	Een audittrail is ingericht waaruit blijkt wie welke data wanneer heeft ingevoerd		
2. Transactie-verwerking	De software leverancier heeft beheersingsmaatregelen getroffen om met een redelijke mate van zekerheid te waarborgen dat de rekenregels de marktwaardeberekening conform het waarderingshandboek uitvoeren	5	Rekenregels van het handboek zijn juist en volledig ingericht in het systeem		
2. Transactie-verwerking		8	De eindgebruiker (woningcorporatie) kan geen rekenregels in de productieomgeving aanpassen		
3. Onderhoud van de bestanden	De software leverancier heeft beheersingsmaatregelen getroffen om met een redelijke mate van zekerheid te waarborgen dat de applicatie de marktwaarden juist, volledig weergeeft	11	Uitkomsten (marktwaarden) kunnen na de berekeningen niet meer aangepast worden		
4. Rapporten genereren		12	Rapporten moeten de volgende identificatiegegevens laten zien: - Datum en tijdstip van het rapport - Titel van het rapport - Paginanummering		
		13	Rapporten moeten de volgende verwerkingsgegevens laten zien: - Selectiecriteria		

Aligning IT with RPA business requirements through COBIT

My mission is to take the Robot out of the human so that we can focus on what really matters

Steven Boekhoudt



Steven Boekhoudt works as a Data Analyst (Auditor & Consultant) and is the Dutch RPA Assurance lead for PwC.

He's passionate about numbers, IT, math and games theory. So it is only logical for him to work within Data Analytics. On a day to day basis he gets the opportunity to solve data related jigsaws.

His main focus area is on **Trusted Robotics** (RPA). He has developed multiple software robots to substitute repetitive straightforward manual process and has setup a RPA CoE with the appropriate governance and a team of developers.

Besides building robots he is experience in assessing the governance of RPA landscapes at large international companies.

1 Introduction

1.1 RPA as an emerging technology (relevance)

PwC (2016b) has analysed more than 150 emerging technologies and concluded that there are the "Essential Eight" that every organization must consider over the next three to seven years to sustain its viability. To arrive at the "Essential Eight", PwC (2016b) evaluated business impact and commercial viability over the next five to seven years (and as little as three to five years in developed economies) and applied the following criteria in its review:

- relevance to companies and industries;
- global reach;
- technical viability, including the potential to become mainstream;
- market share and growth potential; and
- the pace of public and private investment in them PwC (2016b).

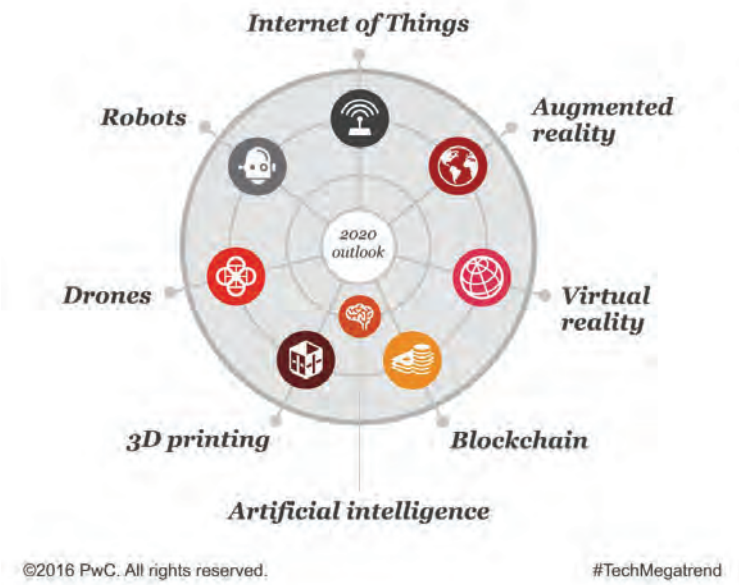


Figure 1 PwC (2016b): The Essential Eight

As shown on figure 1 "Robots" are one of the Essential Eight. Robots are defined herein as RPA. Not only PwC concluded that RPA is one of the essential emerging technologies of today. According to Alberth & Mattern (2017) RPA is a promising automation technology that will become increasingly important and has a huge future potential. It's a non-invasive technology that can improve old business models by incorporating robots into the existing IT landscape and that can be applied to a new digital business model. Alberth & Mattern (2017) claim that the presence of robots within the workspace of organizations is inevitable. Robots will in the near future (and as a matter of fact already are) working along humans, both focusing on their own expertise.

The RPA market share is currently growing at a rapid rate and is estimated to be around $ 1 billion and expected to grow to $ 5 billion in 2022 according to Morrisey, S. (2018). Based on a survey by David Brown et alia (2018) RPA is one of the top positive trends and initiatives for 2018 and beyond.

However, a survey by David Brown (2015 Q2) states, that whereas the cognitive revolution is indeed happening, the immaturity of these advanced technologies, including RPA, poses limits in the short term. Businesses will be wise to avoid false expectations amid the hype. With as key takeaway that the RPA opportunities are plenty but the adaptation by business is challenging. The survey further reveals that one of the reasons for slow adaptation of RPA is due to the immaturity of RPA vendors.
Based upon the most recent report issued by Forrester (2018 Q2) RPA vendors have grown rapidly (especially since the previous report in 2017) and are moving fast. The focus of the RPA software these days is on deployment efficiency, scale, training breadth, new ways of looking at governance and advanced analytics. Since 2015 RPA vendors are quickly "maturing" and their software has advanced in such a way that it has become more reliable (e.g. OCR, cross application selector usages) and easier to use (e.g. drag and drop, recording functionalities).
The Everest Group Research (2018a) underpins that RPA is expected to grow annually at a 75-90% compounding rate due to increasing business awareness, increasing sophistication, expansion in new markets and a positive momentum created by success stories. Although currently buyers are satisfied with RPA vendors, the survey of David Brown (2015 Q2) points out that most buyers are still in their early adaptation phase and will be so for the upcoming years as they continue to test the technology before scaling further. This all leads to the conclusion that the market potential for RPA is huge, is expected to grow and that the software vendors have rapidly matured but that companies are still struggling to scale and to increase their robotics taskforce in order to unleash the full potential of RPA.

1.2 Aligning IT with RPA business requirements (problem)

Everest Group Research (2018a) suggests that the slow adaptation of RPA in the market is due to (1) a lack of RPA knowledge and expertise within the business, (2) companies selecting non-standardized use cases (poor funnel management), (3) unclear ownership (between business and IT), (4) hidden costs and (5) internal resistance.
Gartner (2018) stretches the importance of creating a Joint IT and Business RPA Team. In most businesses, process leaders are (obviously) responsible for completing processes but equally often unaware of what the technology can do and how it can help them. In order to rethink processes by combining it with a new technology like RPA, it is important to have IT engaged.
Another ingredient for a successful adaptation of RPA as suggested by Gartner (2018), is to formalize IT involvement in the early stage of development, so as to maximize positive business outcome. IT teams need to understand why RPA is different from other tools and they also need to know what security and deployment plans are optimal to support evaluating and deploying RPA in its potential to deliver quick, short-term gains through existing user interface pathways. Developing a joint understanding between business and IT will facilitate a much quicker set of results and will enable scaling.
Gartner (2018) then comes up with a list of examples why IT involvement is so essential with respect to RPA. A few examples are:

- Monitoring system changes and performing system maintenance that if overlooked, could adversely impact the bots if they are planned and/or programmed to run 24/7;
- Coordinating security, testing and audit data of the deployment in preproduction and postproduction;
- Discussing any planned IT changes of systems that interact with RPA (API) scripts and keeping scripts up to date;
- Overseeing and incorporating password issuance and refresh strategies to meet business or regulatory compliance in RPA deployments;
- Encouraging coding standards for RPA deployment to avoid suboptimal coding designs and product use.

EY (2018) states that companies think about the initial automation project but forget that RPA will deliver a virtual workforce that allows the business to task robots across the entire organization. IT would not be

in charge of managing the current human workforce, nor should it manage a virtual one. In addition, a business owned RPA Centre of Excellence (CoE) will liberate IT to focus on things that are more valuable. Business led CoE's allow it to prioritize which processes to automate and what the virtual workforce should do. In contrast, IT still has a crucial role in delivering infrastructure and software support, but also to jointly govern and manage change in automated processes.
David Wright, Director, Deloitte (2018) underpins that "IT are absolutely critical to the successful deployment of RPA. This was a lesson we learned early on in our own RPA deployment in Deloitte. I have found there is a significant difference in both speed and cost to deliver between clients that have an engaged and supportive IT function and those where IT is less supportive."
A global online survey by Deloitte (2017) concluded that after the lack of standardisation within the processes the second top challenge for scaling RPA is the buy-in and support from IT. The buy-in is especially important for a successful integration of RPA. The survey further points out that the IT organisation is essential in setting up a scalable and secure infrastructure on which the Robots can be build. Other key roles IT should play are testing systems, approving UAT's and signing off before go-live. After the robots are live and implemented, it is important that IT is involved in monitoring and supporting with incident management (Deloitte (2017)).
In summary, IT and business alignment in the context of RPA is essential to ensure a sustainable RPA taskforce that is able to scale. Because RPA is a so-called IT-lightweight, initiatives start within the business, but to be able to scale across the business IT needs to be on board to plan, organise, implement, maintain and monitor the robots.

1.3 Hypothesis (solution)

I would like to discuss whether COBIT could be an answer to the challenge the market is currently facing with respect to scaling RPA in that IT is usually insufficiently aligned with the business in this area.
COBIT is a widely used framework to align IT and business. It consists of 34 naturally grouped IT control processes, which, if being followed by IT, should align them with the business. However, because RPA is not yet a standard IT solution/application, it is important to examine whether COBIT could be an adequate support framework to achieve the required alignment.
Therefore, my hypothesis is:
Is the application of COBIT 4.1 causing alignment of IT and RPA specific business requirements, as a result of its 34 IT control processes addressing the RPA specific risks?

To answer the above hypothesis, the following questions will be addressed:
- What is Robotics Process Automation (RPA)?
- What is RPA specific risks?
- Are the RPA specific risks addressed by COBIT?
- Case Study: does COBIT mitigate the RPA specific risks to align IT and business?
- Conclusion: does COBIT mitigate the RPA Specific risks to align IT and business?

First and foremost, however, I will elaborate on the methodology applied in this thesis.

2 What is Robotics Process Automation?

2.1 Definition of RPA

Let's start by defining what Robotics Process Automation (RPA) is. Lacity et al. (2015) refer to RPA as software systems that are configured to execute rules-based, repetitive tasks, which were previously performed manually. Alberth & Mattern (2017) give another definition, that considers RPA to be a virtual workforce in the form of software that can mimic a human worker executing a transaction or a particular process.

The Institute for Robotic Process Automation & Artificial Intelligence (IRPAAI) (2018) defines RPA as “the application of technology that allows employees in a company to configure computer software or a “robot” to capture and interpret existing applications for processing a transaction, manipulating data, triggering responses and communicating with other digital systems”.
Gartner (2018) defines RPA as a tool designed to mimic the same "manual" paths taken by a human, by using a combination of user interface (UI) interaction. An RPA tool operates by mapping a process for the software "robot" to follow computer pathways and various data repositories, so the RPA can operate in place of a human. An RPA tool triggers manually or automatically, a movement or population of data between prescribed locations, documents audit trails, conducts calculations, performs actions and/or triggers “downstream” activities.
There are many more definitions but all of them seem to underpin that RPA is software, that can be configured to execute certain tasks and that has the ability to execute across multiple (existing) applications. Therefore one could claim that the IT department of a company is key in enabling a successful adoption of RPA.
On the other hand, one could deduct from the different definitions, that RPA mimics human behaviour by being business and rules-based. Therefore, an in-depth understanding of the business and its processes is key in building the robots or at least in conceptually designing the robots properly.
In the context of adopting and scaling RPA the collaboration and mutual understanding between IT and business is essential. On the one hand business needs to define what the robots conceptually must do within certain processes, whereas on the other hand IT needs to plan, implement, maintain and monitor the robots.

2.2 What are the benefits of RPA?

As shown on figure 3 below, one could think of multiple benefits arising from RPA and therefore good reasons why RPA is one of the current emerging technologies. RPA software is non-invasive and has a quick ROI. Organizations do not have to alter their current IT landscape to enable it. The robots utilise so-called “selectors” to act across current existing applications, which makes it possible to substitute standardized processes performed on a computer thereby increasing productivity while reducing cost by substituting hours spent by FTE’s.
Another crucial benefit of robots relates to the fact that they always perform the tasks in the same way. Therefore, the risk of human errors is zero, which decreases the chances of non-compliance for an organization as a whole as a result of (individual) human mistakes. Moreover, robots are available to do the work day and night, on weekends and during holidays. Other key benefits are illustrated in figure 3.

Figure 3 Source: Infosys

3 What are RPA specific risks?

To get a complete set of RPA related risks I conducted a thorough literature study by combining RPA risk related articles published by Deloitte, EY, KPMG, PWC, RPA vendors and specialists. All the relevant RPA risks where subsequently consolidated and then clustered per domain to collate the top RPA risks. The below subchapters provide a brief description of each risk domain.

3.1 R1 Change Management

As emanates from the definition of RPA given the interaction with humans, the graphical user interface plays a key role. In other words, the programmed robots make use of what can be seen on the screen. With so-called "selectors" they typically identify parts of the screen visible to humans and are learned to perform actions. When these visual parts of the screen change, it potentially could lead to a break-down of the robots. For example, when the colour of a button changes, the Robot may stop working or even worse, will keep performing a task but will be doing the wrong things (false positives).

3.2 R2 Talent & Capabilities

Building robots is a joined effort of people from multiple disciplines. Companies should have experts that understand the process, RPA developers that build the robots and IT that supports this collaborative process. Now imagine a company scaling their RPA programme in order to decrease the manual labour and to reduce the number of FTE's. This means a lot of change in the way a company works and increases the work pressure on those that are responsible for organizing, implementing, maintaining and monitoring the robots as well as the ongoing business operations. When managing a digital task force instead of a human led taskforce, the talent and capabilities to do so changes. The robots need to be build maintained and monitored. In addition, who is accepting responsibility when changing from a human to a digital taskforce?

3.3 R3 Overdependence on Key Resources

The idea of RPA is to create a digital workforce to (in theory) substitute standardized manual tasks. If only a few key personnel manage this digital robots' workforce, how do organizations address business continuity when one departs?

3.4 R4 Systematic Errors

One of the benefits of using robots is that they solve the problem of human errors. The robots structurally and without any exceptions perform a process in the same way. However, when a robot does make an error because of e.g. a missed change, a flaw in the design or an unforeseen exception in the process, that error becomes systematic and could spread within the organization like a fire. Therefore, where there was previously the risk of a human error now there is a risk of systematic error.

3.5 R5 Access Management

Robots, like humans, will login to systems and be able to store or retrieve data from applications, portals and/or other systems. In order for a Robot to do so, it needs access by having the right credentials at its disposal. However, developers or anybody else in the organisation that have access to the robots, automatically "inherit" the robot's access rights. So how do companies ensure that there is sufficient segregation of duties and to mitigate the risk of unauthorized access to their IT landscape through Robots? This challenge gets bigger when the RPA program spreads in the organisation.

3.6 R6 Monitoring

Robots can be run locally on a laptop (because of access rights) or on one or more VDI environments (to avoid clashes). They can be distributed decentral throughout the whole organisation. How would a company be able to monitor these robots on their operational effectiveness and performance?

3.7 R7 Robot Design Quality

There are many ways to build the same robot. Meaning that the outcome of different robots could be the same but their creation could differ. A simple example could be that the variables in the code were not given meaningful names, which leads to poor readability and makes it difficult to implement changes.
In other words, the quality of the design of the robots can differ substantially. This is especially true in an environment where there are many developers, which is not unthinkable with RPA because it has been made fairly easy to program a simple robot (most software packages have graphical supporting UI with e.g. drag-drop or recording functionalities). When scaling an RPA programme in most cases multiple developers will do the work. How will a company ensure the quality of the design of the Robots?
Uipath (2018) addresses the following key design principles to ensure an acceptable quality:

- Flexibility (keep environment settings in external configuration file);
- Credentials should be externally saved in a safe (not in the design);
- Readability (meaningful names, annotations);
- Maintainability (good structure and development standards, in order to effectively change robots if needed);
- Reliability (exception handling and error reporting should be embedded)

3.8 R8 Non-Compliance

Because robots will probably have access to multiple applications and potentially handle sensitive data with build-in credentials, how do you ensure compliance? Is there an audit trail that always points at the person responsible? Do you know what all the robots are doing when they are spread over the organisation?

3.9 R9 Funnel Management

Deciding which use case to select to robotize is essential. Before building robots an organization needs to know if it's a standardised process and if there are other ways of automation that are more effective for example. One has to understand if the applications in scope are stable enough (change management). During the "use case selection phase", a company should estimate the total costs of building, implementing and maintaining robots and assess whether or not these are lower than the expected benefits. Funnel management or selecting and prioritizing robot use cases is fundamental and complex. Therefore very important to be done as a joint effort between IT and business.

3.10 R10 Deployment Strategy

One of the key benefits of RPA is that it is a non-invasive technology that could be used on top of an existing IT landscape. Robots can perform actions over multiple applications based on the graphical user interface. How will an organisation test and deploy robots if it "sits upon" the existing IT landscape? Is there a test environment present that exactly mirrors this landscape with test data? In practice this especially difficult because Robots are mostly being used in relation to legacy or older applications that do not interface well. How does an organisation deploy these robots and perform UAT's while staying sufficiently agile?

3.11 R11 Unclear Roles and Responsibilities

Because robotics is an IT-lightweight solution, initiatives mostly start in the business and then organically grow (bottom-up). However, when scaling, IT becomes increasingly important to organize, maintain and monitor the robots (think of access to different applications by robots). So, who owns the RPA programme

and who is responsible for all these different tasks? Who is responsible for the credentials that robots use to access systems?

3.12 Summary RPA specific Risks

In the below illustrated table 1 all the previously discussed RPA risks are summarized.

Risk description	Risk number
Robots make use of the graphical user interface. When the graphical interfaces change the Robot could potentially break down or worse might create false positives. So how do you implement GUI changes while potentially hundreds of robots are spread through the organization?	R1 Change Management
When managing a digital taskforce instead of a human led taskforce the necessary talent and capabilities change. The robots need to be built, maintained and monitored. Even more, who is going to be tasked with these activities when changing to a digital taskforce?	R2 Talent & Capabilities
The idea of RPA is to create a digital workforce. If only a few key personnel manage these robots how do you address business continuity of a departure?	R3 Overdependence on key resources
The advantage of using robots is fewer human errors at the expense of systematic errors. Errors could become widespread across business processes. How will you cope with these new types of errors?	R4 Systematic Errors
Robots are being used to interface between systems and/or applications via the GUI, robots will need access to credentials to these systems. How will a company ensure no misuse of these credentials by developers?	R5 Access Management
Robots will perform different steps over multiple systems, how do you monitor operating effectiveness especially when there are many robots?	R6 Monitoring
Robots can be designed in many different ways with different quality standards. Especially because building robots has been made relatively easy, developers don't have to have a solid programming background. How do you ensure that the quality of design is sufficient?	R7 Robot Design Quality
Because robots will have access to multiple applications and potentially handle sensitive data, with build-in credentials, how do ensure compliance? Is there an audit trail that always points to a responsible person?	R8 Non-Compliance
Deciding which use case to select to robotize is essential. At incubation you have to know if it's a standardized process but among other things also if the applications are stable enough (change management). So, who is in charge of funnel management?	R9 Funnel Management
Robots can perform actions over multiple applications based on the GUI. How will an organisation test and deploy robots if it sits upon the existing IT landscape? Is there a test environment present that exactly mirrors this landscape with test data?	R10 Deployment Strategy
Because robotics is an IT-lightweight product, initiatives mostly start in the business. However, when scaling RPA, IT becomes increasingly	R11 Roles & Responsibilities

important to organize, maintain and monitor the robots (think of access to different applications by robots). So, who owns the RPA programme and who is responsible for what?

Table 1 Summary of RPA specific risks

4 Are the RPA specific risks addressed by COBIT?

Building robots is a joint effort between IT and business. Mostly the people that come from the business are acquainted with the processes that can be robotized but IT for example is capable of managing the authentication of robots. The focus in this part is on whether the IT control processes address the RPA related risks.
First, a brief introduction to COBIT will be given and then for all the separate 34 COBIT IT control processes the purpose and control activities will be described. Based on this description of the control activities and the RPA defined risks, a mapping will be made, and a conclusion drawn on whether the activity addresses an RPA specific risk.

4.1 Mapping of the specific RPA risks to 34 IT control processes of COBIT

In this Chapter all the 34 IT control processes will be described and analysed as to whether they address RPA specific risks. COBIT 4.1. is divided into four domains. As illustrated by Figure 4 COBIT 4.1. Each phase will be briefly explained and thereafter the IT control processes will be discussed in more detail.

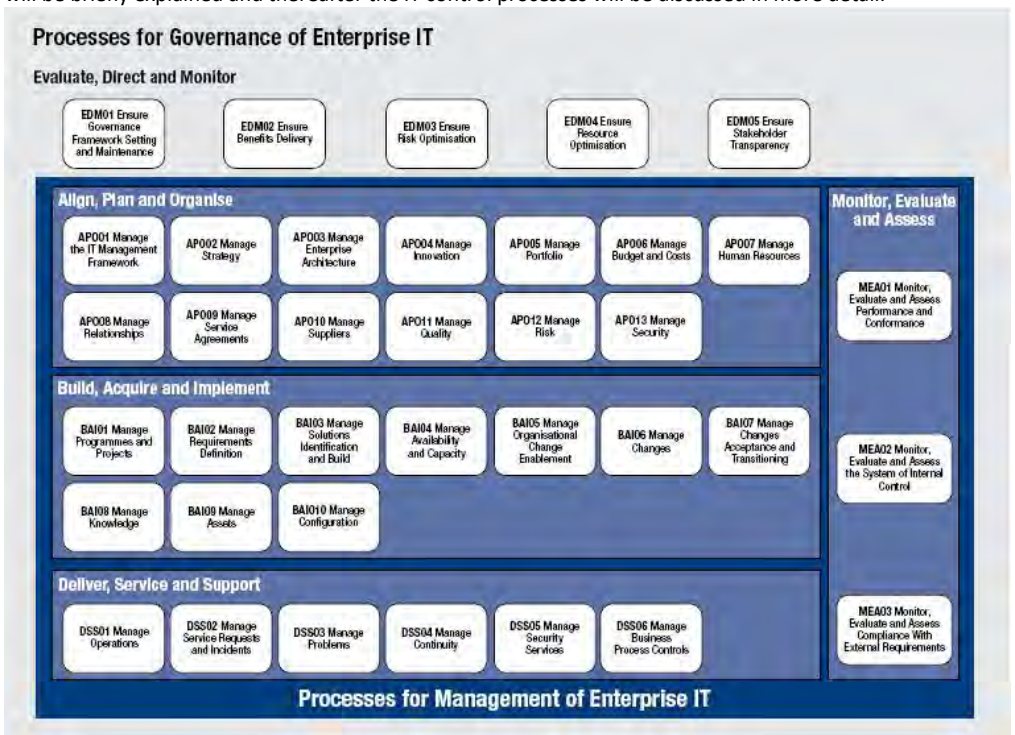


Figure 4 COBIT 4.1 framework

4.2 Conclusion

As summarized in the below table 2, apart from some nuances, COBIT 4.1 addresses all of the RPA specific risks. Consequently, in theory COBIT 4.1 could be an adequate framework to align IT with RPA business requirements.

The first nuance is that building robots is a joint effort between IT and business anyway therefore R3 Over-dependence on Key Resources and R2 Talent & Capabilities should be mitigated not only for IT but also for the business. Because the hypothesis in this thesis is about aligning IT and business, such factual partnering between IT and business does not lead to a negative or different conclusion.

The second nuance relates to the R7 Robot Design Quality, which could be part of the IT control process DS9 but is not very explicitly addressed therein. However, ensuring the quality of the robots is very important when scaling. Maintainability and readability of the robot code are key elements to effectively implementing changes for example.

RPA Risk	Comments	IT control process	Conclusion
R1 Change Management	The risk is addressed however from a practical standpoint it is still challenging to manage	AI6	Addressed
R2 Talent & Capabilities	From an IT perspective this Risk is addressed for RPA. However, these controls should also be present in the business to fully mitigate the risk.	PO7, AI4, AI5, DS3, DS7	Addressed for IT
R3 Overdependence on Key Resources	From an IT perspective this Risk is addressed for RPA. However, these controls should also be present in the business to fully mitigate the risk.	PO7, AI4, DS7	Addressed for IT
R4 Systematic Errors	This risk is addressed however from a practical point of view this still could lead to challenges.	DS4, DS8, DS10	Addressed
R5 Access Management	This risk is addressed and when the risk is understood could be mitigated by IT.	DS5	Addressed
R6 Monitoring	Monitoring robots that are spread-out in the organisation is a challenge. IT could assist by coming up with a technical solution to centrally monitoring the robots.	PO8, P10, DS8	Addressed
R7 Robot Design Quality	This risk is addressed if the integrity of the configuration and it can be translated into the quality of the robot design.	DS9	Could be addressed
R8 Non-Compliance	This Risk is addressed by COBIT from an IT perspective, so	PO6, DS5, ME3	Addressed

	this partially depends on their responsibilities.		
R9 Funnel Management	Business and IT should be aligned with respect to selecting and prioritizing robots. If this is addressed in PO1 the risk is covered.	PO1, PO5	Addressed
R10 Deployment Strategy	If IT ensures proper Dev, Test and Prod environments that are exactly alike from a UI perspective this risk could be mitigated.	AI2, AI3, AI7	Addressed
R11 Unclear Roles and Responsibilities	This Risk is addressed by COBIT, which will help the business implicitly to define their roles and responsibilities.	PO2, PO4, DS1	Addressed

Table 2 Summary of Mapping

5 Case Study: does COBIT 4.1 mitigate the RPA specific risks to align IT and business?

In this Chapter, the results and findings of an RPA specific audit are discussed in order to reflect on the findings of the previous Chapter. The audit was performed within an organization that adopted COBIT 4.1. Because the final report is still being used internally, the results cannot be made public and neither the identity of the company nor the related audit documentation will be shared herein.

5.1 Theoretical risk/control framework

After closely studying the RPA risk literature (Chapter 3) the below risk/control framework was constructed. The five domains and sub topics cover all the RPA risks and where discussed internally (within PwC) with Internal Audit & ITGC experts. Behind every topic, there are several control hypotheses and questions specified for the organisation, because depending on their RPA strategy, the questions may differ although many of the underlying topics remain. Altogether, this served as the basis for the RPA specific audit. Unfortunately, because the detailed framework was a co-creation and part of the actual audit performed, the documentation is not part of this thesis.

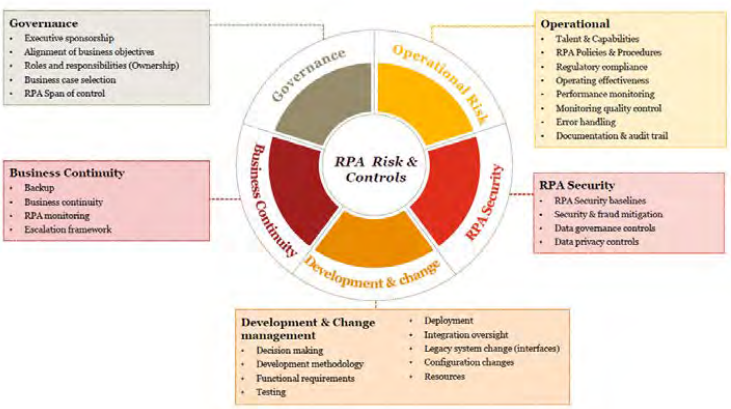


Figure 5 case study control framework

Either implicitly or explicitly all the eleven RPA risks are being addressed. The difference in wording is a result of the terminology the organisation applied in the case study. Just to ensure that there are no misunderstandings, the more implicit risks are:

- R9 Funnel Management which is the same as business case selection
- R3 Overdependence on Key Resource and R4 Systemic Errors are addressed within business continuity
- R7 Robot Design Quality is addressed in development methodology
- R5 Access Management is addressed in RPA security part

Besides the RPA specific risks discussed in Chapter 3, other topics were also in scope. Documentation & audit trail is an important topic to discuss but was more specifically related to having an Agile Scrum way of working and not so much to the RPA technology itself. Therefore, this was not discussed in Chapter 3 but it is important to address for the organisation in the case study.

Executive sponsorship also not addressed in Chapter 3, is in scope in the case study. It is an essential topic within RPA because in most cases the initiatives start in operations or with people that are performing the standardised tasks. However, if there is no top-to-bottom sponsorship, the likelihood of an RPA program effectively scaling throughout the organization is decreasing.

The domains and sub topics are further translated in control questions, which form the basis of the interviews with all the key stakeholders. Either the question came from COBIT 4.1, were derived from the literature, internal expertise or from close cooperation with the organisation. For example, in case of Funnel Management the questions were:

- What is the formal methodology to inventory, analyse and prioritise that is in place and how is it documente? to ensure that only RPA projects with beneficial impact on the organization?
- Who is responsible to identify suitable processes for RPA and how is this done?
- How is it ensured to identify all use case?
- Who is responsible for prioritizing the use cases and defining their business case and how is this done?
- Are these processes optimized before we automate and/or robotise?
- Who is responsible for feasibility assessments and how are these performed?
- Who decides in which process RPA will be deployed?

5.2 Findings

After a month of interviews, discussions and litrature studies, together with Internal Audit a report with findings was issued. The most important findings were:

1 An overall Risk Assessment was performend on RPA. Altough it adressed some important risks like R2 Talent & Capabilities and R3 Overdepence on Key Personnel it missed several other important risks such as R4 Systemic Errors, R1 Change Mangement and R7 Robot Design Quality. Conclusion was that the stakeholders that performed the risk assessment didn't have enough RPA knowledge at the time.

2 Initially we were informed that change management was part of the ITGC's and therefore adressed. However change management was not adjusted for RPA (no centralized RPA control room) already leading to a few incidents where multiple robots broke down at once as a result of a software updates. (R1 Change Mangement)

3 Monitoring the operating effectiveness of robots in production was still in progress and not yet performed. Mostly due to techinical challenges of implementing Kibana (off the shelve RPA monitoring tool). However, even if they implemented Kibana to monitor the operating effectiveness, Kibana only reports on wheter or not the robots performed their steps succesfully. Kibana therefore is unable to detect false positives. (R6 Monitoring)

4 After performing a code review on serveral robots we came to the conclusion that there were no explicit design principles that enforce a base quality with respect to the design of the robot. This led to poor readability and maintainability among other things. (R7 Robot Design Quality)

5 Selecting use cases was done with as key focus on reducing FTE's. By not adressing the inherent risks of RPA and or other means of automation the robots that were build either had low value-added or broke down quickly when entering production. (R9 Funnel Management)
6 There was a RACI in place which clearly describes all the roles and responsiblities of people involved with RPA. (R11 Unclear Roles and Responsibilities)
7 The risks of access management were mitigated by having a clear development, test and production envirnoment with corresponding credentials. When robots entered production the credentials where changed by the admin who had no access to the code of the robots in production (SOD). (R5 Access management and R10 Deployment Strategy)
8 A compliance officer was appointed as part of the team that performs the final UAT. (R8 Non-Compliance)
9 A Center of Excellence for RPA was being set-up in order to create a team of experts. (R2 Talent & Capabilities and Overdependence on Key Resources)

5.3 Conclusion

The final advice of the report was to cease to build robots and first address the above-mentioned issues. The main strategy was to reduce FTE's by building robots. However, because these robots are not built in a trustworthy manner the risk arose of laying off people, while having an unreliable robotics taskforce to replace them as part of their core processes. Even though the organisation uses COBIT 4.1 this was the main conclusion. The most important reason why COBIT 4.1 did not cover the RPA specific risks is because the performed risk assessment, as part of COBIT 4.1 process PO9, failed to bring them forward.

The reason why the risk assessment did not uncover the RPA risks is mostly due to not having the knowledge at that time of RPA. As shown in Chapter 3 most of the sources used in this thesis are either from 2017 or 2018. Therefore, one could conclude that RPA is still an emerging technology and therefore not a lot of benchmark material is available and some risks were simply not understood. During the root-cause analysis phase this was further confirmed. A lack of knowledge was the main reason as to why the findings came to bear in the first place, even though the organisation follows COBIT 4.1.

An example of where knowledge lacked was with respect to R1 Change Management. The organisation thought change management was addressed by the existing ITGC's. However, when taken a closer look it still had to be adjusted for RPA. IT had no central oversight and was not able to measure the impact on all existing robots in the organisation, let alone be able to effectively implement changes, even though COBIT 4.1 explicitly addresses change management. Other examples of risks that could have been covered but were in fact not, are R6 Monitoring and R4 Systemic Errors (finding 3 & 4).

Secondly, as described in the conclusion of the previous Chapter 4, the concern with respect to COBIT 4.1 addressing the risk of R7 Robot Design Quality is justified by the case study results. There were no quality standards with respect to building the robots by the developers. When scaling this could become a real problem as the robots are not designed to be maintained. Furthermore, there are no controls build into the design of the robot so that the Kibana report can effectively monitor false positives. Therefore, this should be made explicit in IT control process DS9.

Thirdly, even though a formal R9 Funnel Management was setup like COBIT 4.1 describes, because the overall strategy was only focussing on reducing FTE's, selecting and prioritizing of robot use cases was done poorly. For example, maintaining the robots was not part of selecting the use cases and consequently most robots broke down in the live production environment. Lesson learned therefore, is to not only focus on the reduction of FTE's but to also address the full picture of costs (e.g. maintenance, alternatives way of automation) and benefits of Robots (e.g. fewer human errors, reduction of peak workload). However, this could also be a result due to lack of proper RPA knowledge and understanding.

6 Conclusion: does COBIT mitigate the RPA specific risks to align IT and business?

In theory COBIT 4.1 addresses the specific risks that arise from implementing and scaling an RPA programme. With some common robot design principles to ensure quality and maintainability of the robots, COBIT 4.1 could serve as a framework to align IT with RPA business requirements, which would support organisations in scaling and releasing the full potential of RPA. Based upon the literature eleven specific RPA risks were identified. Going through all the 34 IT control processes of COBIT 4.1 all the risks were addressed with a few nuances.

The first nuance is that building robots is a joint effort between IT and business therefore R3 Overdependence on Key Resources and R2 Talent & Capabilities should be mitigated not only for IT but also for the business. Because the hypothesis (Chapter 1.3) of this thesis is about aligning IT and business this does not lead to a negative conclusion. Second nuance is regarding the R7 Robot Design Quality, which could be part of the IT control process DS9 but is not very explicitly addressed. However, ensuring the quality of the robots is very important when scaling. Maintainability and readability of the robot code are key elements to effectively implementing changes for example.

However, when putting COBIT 4.1 to practice we learned that in the context of RPA, I did not fully address these risks. Mostly because RPA is an emerging technology which led to the lack of expertise and proper knowledge to perform the initial risk assessments, set the right strategy and select & prioritize the right use cases. By focussing on FTE's reduction and not uncovering RPA specific risks the organisation was susceptible to unknown but great risks.

From the case study one could conclude that having the right RPA knowledge is essential to use COBIT 4.1. The most important reason why COBIT 4.1 not fully covered all the RPA specific risks in the case study is because the risk assessment performed, as part of COBIT 4.1 process PO9, was unable to unravel the RPA risks. As shown in Chapter 3 most of the sources used in this thesis are either from 2017 or 2018. Therefore, one could conclude that RPA is still an emerging technology and therefore not a lot of benchmark material is available. During the root-cause analyses phase this was further confirmed. A lack of knowledge was the main reason as to why the findings came to exist in the first place even though the organisation follows COBIT 4.1.

This all leads to the overall conclusion that although COBIT 4.1 in theory is an adequate framework to align IT and RPA business requirements one should consider if there is enough knowledge and expertise to apply COBIT 4.1. RPA is a new and emerging technology with new and specific risks. These risks should be fully considered when applying COBIT 4.1 and only then will it align IT and business.

7 Literature

- Alberth, M., & Mattern, M. (2017). Understanding robotic process automation (RPA). Automation, 54.
- Davenport, T.H., & Kirby, J. (2015). Beyond automation. Harvard Business Review, 93(6), 59-65.
- David Brown, Bob Cecil, Jo Page, Stan Lepeak (2018). Adoption of intelligent automation does not equal success, 4th Quarter 2017 KPMG Global Insights Pulse Survey Report
- David Brown (2015 Q2). Robotic Revolution – separating hype from reality Key Findings from KPMG's 2Q15 Global Sourcing Advisory Pulse Survey.
- Deloitte (2017). The Robots are ready. Are You? Untapped advantage in your digital Consulting.
- EY (2018). Get ready for robots. Why planning makes the difference between success and disappointment.
- Everest Grourp Reserarch (2018a). Robotic Process Automation (RPA) Annual Report 2018 – Creating Business Value in a Digital-First World.
- Everest Grourp Reserarch (2018b). Enterprise RPA Adoption | Pinnacle Model Assessment Overview.
- Gartner (2018). Robotic Process Automation: Eight Guidelines for Effective Results.
- IT Governance Institute (2007). COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models. ISBN 1-933284-72-2
- Institute for Robotic Process Automation & Artificial Intelligence. (2018). What is Robotic Process Automation? IRPAAI.
- Investopedia. (2018). Robotic Process Automation (RPA).
- Lacity, M., & Willcocks, L. (2015). What knowledge workers stand to gain from automation. Harv. Bus. Rev, 19.
- Lacity, M., Willcocks, L. P., & Craig, A. (2015). Robotic process automation at Telefonica O2.
- Le Clair, C., Cullen, A., & King, M. (2017). The Forrester Wave™: Robotic Process Automation, Q1 2017.
- Le Clair, C. (2018). The Forrester Wave™: Robotic Process Automation, Q2 2018.
- Leemhorst, L. (2017). The impact van Robotics. The Next Generation. IIA Congres 2017. Retrieved from https://www.iia.nl/SiteFiles/IIA%20Congres/2017/Presentaties/Lars%20Leemhorst%20web.pdf
- Willcocks, L. and Lhuer, X. (2017). The value of robotic process automation. McKinsey & Company. Retrieved 30 May 2018, from https://www.mckinsey.com/industries/financial-services/our-insights/thevalue-of-robotic-process-automation
- Willcocks, L. P., Lacity, M., & Craig, A. (2015). The IT function and robotic process automation
- PwC. (2015). Tijdwinst met behulp van robotisering dataverwerking. PwC. Retrieved 21 February 2018, from https://www.pwc.nl/nl/themas/digital/klantcases/financiele-dienstverlener.html
- PwC. (2016). Organize your future with robotic process automation. PwC. Retrieved 21 February 2018, from https://www.pwc.com/us/en/operations-management/publications/robotics-process-automation.htm
- PwC (2016b). What are the essential eight technologies? PwC retrieved on 15-9-2018 from http://usblogs.pwc.com/emerging-technology/a-guide-to-the-essential-eight-emerging-technologies/
- PwC. (2017a). Robotic Process Automation (RPA): A primer for internal audit professionals. PwC. Retrieved 21 February 2018, from https://www.pwc.com/us/en/risk-assurance/publications/roboticprocess-automation-internal-audit.html
- PwC. (2017b). Spotlight: Robotic Process Automation (RPA). (2017). Tax Function Of The Future. Retrieved from https://www.pwc.com/gx/en/tax/publications/assets/pwc-tax-function-of-the-future-focuson-today-robotics-process-automation.pdf\
- Ransbotham, S., Kiron, D., Gerbert, P., & Reeves, M. (2017). Reshaping business with artificial intelligence. MIT Sloan Management Review, 59(1).

- Shacklett, M. (2015). Business process automation: Where it works, and where it doesn't | ZDNet. Retrieved from https://www.zdnet.com/article/business-process-automation-where-it-works-and-where-it-doesnt/
- Uipath (2018). Best practices guide.
- Morrisey, S. (2018). Robotic Process Automation Industry forecast, MEDICI Research And Markets, Grand View Reserach, Worl Economics Forum. Retrieved from https://cdn.interquest-group.com/files/rpa-market-growth-2024-datasheet.pdf
- Zaharia-Radulescu, A. M., Pricop, C. L., Shuleski, D., & Ioan, A. C. (2017). Rpa And The Future Of Work-force. In Proceedings of the International Management Conference (Vol. 11, No. 1, pp. 384-392). Fa-culty of Management, Academy of Economic Studies, Bucharest, Romania.

Blockchaintoepassing binnen de overheid

Kan blockchaintechnologie procesbeheersing vereenvoudigen?

Michiel Daalder

Michiel heeft bedrijfskunde gestudeerd aan de VU, is financieel adviseur, en heeft in 2018 de opleiding IT-audit Compliance & Advisory afgerond. Hij werkt momenteel als ZZP-er in de projectbeheersing op grote infraprojecten en daarnaast bij een infraprogramma bij Rijkswaterstaat. Binnen het programma is hij onder meer betrokken bij de implementatie van een nieuwe werkstroom en bijbehorende IT-voorzieningen binnen de organisatie.
Hiervoor was hij als adviseur werkzaam bij een ingenieursbureau waar hij tevens opdrachten in de projectbeheersing en projectmanagement heeft uitgevoerd.

1 Inleiding

1.1 Introductie

Sinds enkele jaren is de Blockchain als nieuwe technologie binnen de IT in opkomst, maar pas met de recentelijke doorbraak van de Bitcoin is het bekend geworden onder het grotere publiek en wordt de volledige reikwijdte ervan pas inzichtelijk. Blockchaintechnologie staat momenteel in de top 10 van strategische technologietrends (Gartner, 2018). De technologie is een combinatie van bestaande technologieën zoals encryptie, netwerken via internet, voorwaardelijke instructies, computerkracht, etc. Pas nadat deze technologieën een voldoende volwassenheidsniveau bereikt hadden, kon de Blockchain als gecombineerde technologie met toegevoegde waarde geïntroduceerd worden. De technologie bevat kenmerken die uitermate geschikt zijn om verbeteringen te realiseren in informationele zelfbeschikking, processen en zelfs samenlevingen (Swan, 2015). Waar internet op een laagdrempelige manier wereldwijde verspreiding van informatie mogelijk maakt, kan de Blockchain wereldwijde verspreiding van waarde en applicaties bewerkstelligen. Daarom wordt de technologie, na computers, internet en smartphones, vaak de volgende disruptieve innovatie genoemd wordt (Pilkington, 2015; McKinsey, 2016; Gartner, 2018). Enkele belangrijke kenmerken van Blockchain zijn voorspelbaarheid, onveranderlijkheid, veiligheid en het gebruikmaken van één gesynchroniseerde database. Die kenmerken leiden allemaal naar één toegevoegde waarde, namelijk het leveren van vertrouwen tussen alle partijen in het netwerk en daarmee in het proces. Sommige experts twijfelen echter aan het disruptieve karakter. De voornaamste reden hiervoor is dat ze Blockchain als een basistechnologie zien, die een adoptietijd nodig heeft om door organisatorische en sociale barrières heen te breken (Lansiti, M., Lakhani, K.R. 2017). Zij vergelijken Blockchain met het TCP/IP systeem, dat decennia nodig had om door te breken. Deze scriptie laat de menselijke kant echter buiten beschouwing en richt zich op de mogelijkheden tot procesoptimalisatie puur gezien vanuit het instrumenteel perspectief.

1.2 Aanleiding

Veel informatie- en transactieprocessen worden door trends, zoals globalisering, externe bedreigingen en al maar strengere wet en regelgeving steeds complexer. Dit gaat bij deze (hoog compliant) processen ten koste van transparantie en efficiëntie. De verhoogde complexiteit brengt weer nieuwe risico's met zich mee. Om compliant te blijven, zijn dan ook steeds meer beheersmaatregelen nodig, wat de processen nog weer inefficiënter en complexer maakt. Voorbeelden van belangrijke beheersmaatregelen zijn de garantie van een integere transactie of chronologische vastlegging van informatie inclusief koppeling van eigenaarschap. Blockchaintechnologie is in staat de integere uitvoering en vastlegging van een transactie te garanderen op een eenduidige transparante wijze. Het automatiseert en vereenvoudigt daarmee de beheersmaatregel van de vertrouwde intermediair, of kan deze zelfs compleet overnemen zoals bij de Bitcoin het geval is. Door de toegepaste encryptie in de Blockchain wordt er chronologisch een onwijzigbare geschiedenis gecreëerd, gekoppeld aan een identiteit en alleen met toestemming van die identiteit via toevoegingen te actualiseren. Extra maatregelen ten behoeve van data-logging worden daarmee overbodig. Kortom, de Blockchain lijkt te kunnen helpen met het ondervangen en reduceren van beheersmaatregelen.

1.3 Vraagstelling

De bovenstaande uiteenzetting van problematiek en mogelijke blockchaintoepassingen leidt tot de volgende onderzoeksvraag en deelvragen

A. In hoeverre kan een hoog compliant proces geoptimaliseerd worden door toepassing van blockchaintechnologie?

Deelvragen

A1. Hoe is blockchaintechnologie opgebouwd en wat zijn onderscheidende kenmerken? (H2)

A2. Hoe kan met blockchaintechnologieprocesoptimalisatie bereikt worden? (H3)

A3. Hoe is het casestudyproces nu ingericht en gepositioneerd? (H4)
A4. Past blockchaintechnologie op het casestudyproces en is optimalisatie mogelijk? (H5)

In onderstaand model is de onderzoeksvraag gevisualiseerd:

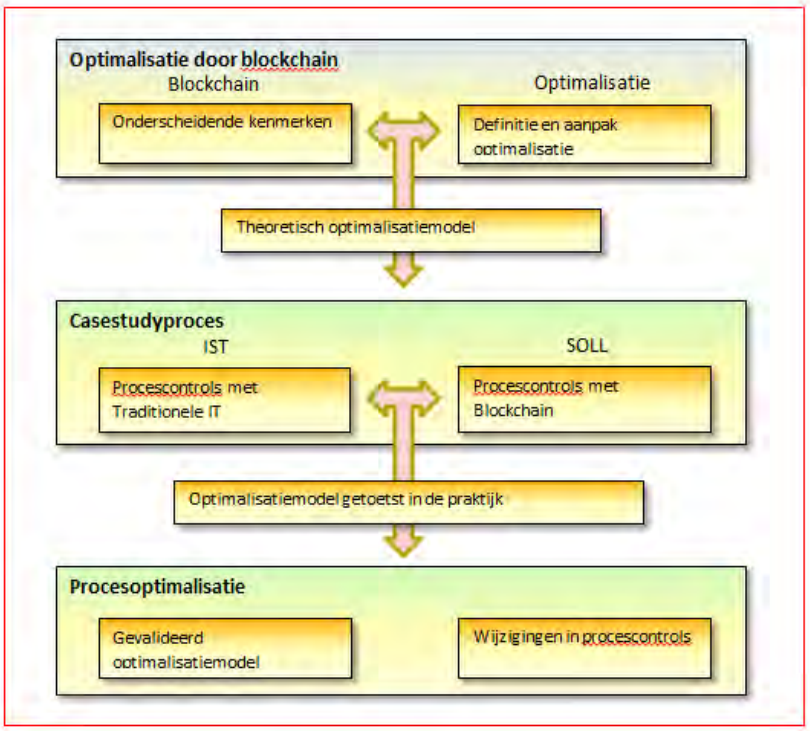


Fig.1 Visualisatie onderzoeksvraag

1.4 Afbakening

De objectscope van de onderzoeksvraag betreft een casestudyproces dat hoog compliant is. In dit onderzoek wordt alleen de case-specifieke norm meegenomen, met daarin de relevante wet- en regelgeving verwerkt. Privacy wordt ook meegenomen bij de afweging van de te kiezen Blockchainvorm, dit is hierbij namelijk een essentieel issue. Het proces wordt in Hoofdstuk 4 verder uitgewerkt en toegelicht.

De IT-omgeving wordt geïsoleerd bekeken, directe invloed door raakvlakken met andere IT-toepassingen worden in dit onderzoek buiten beschouwing gelaten. De architectuur van de te onderzoeken IT-toepassing kan deels gezien worden als die van de standaard opbouw van een Database management System (DBMS). Het systeemlandschap van een DBMS is globaal conform drie lagen opgebouwd, deze lagen kunnen native of via multitier-architectuur opgebouwd zijn. De bovenste laag is de functionele laag, de lagen database en operating system behoren tot de technische laag. Het operating system valt buiten de scope.

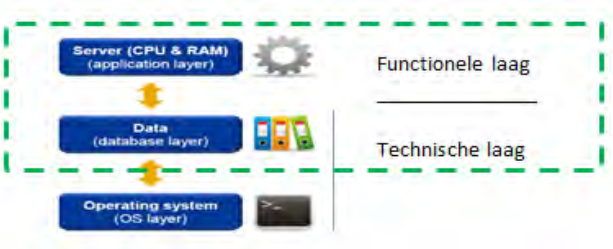


Fig.2 scope binnen systeemlandschap (bron KPMG)

Het onderzoek richt zich primair op het applicationlevel, en direct op het proces. Er is alleen gekeken naar de operationele maatregelen, en niet naar maatregelen op tactisch en strategisch niveau. Verder blijven soft-controls buiten beschouwing en wordt alleen naar hard-controls gekeken.

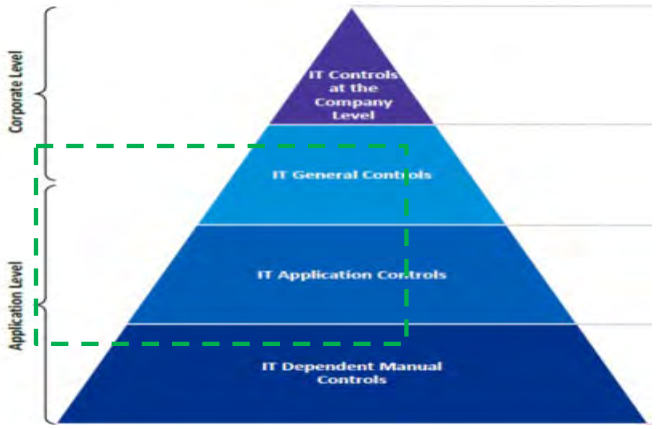


Fig.3 Weergave scope controls (bron: KPMG)

1.5 Uitsluitingen, uitgangspunten en randvoorwaarden onderzoeksobject?

Daarnaast moet aan enkele randvoorwaarden voldaan worden die niet direct op het casestudyproces van toepassing zijn maar wel nodig zijn om het proces adequaat te laten werken. Het voldoen aan wet en regelgeving buiten de norm wordt buiten beschouwing gelaten. Een goed werkende IT-organisatie met de benodigde ITGC's is een randvoorwaarde. Noodzakelijke mutaties in de beheersmaatregelen op ITGCniveau vallen buiten de scope, maar worden wel als aandachtpunt meegenomen. Uitgangspunt is verder dat een succesvolle migratie alleen mogelijk is wanneer er betrokkenheid van het management is en er voldoende middelen ter beschikking gesteld worden. Dit geldt voor alle betrokken partijen, waarbij zij zich tevens dienen te conformeren aan een eenduidige werkwijze en administratie, en macht moeten afstaan. Gezien het relatief snelle verloop in de ontwikkelingen op blockchaingebied, wordt de situatie zoals deze zich in april 2018 voordoet als standlijn aangehouden. Latere externe ontwikkelingen van invloed zijnde op de technologie worden derhalve buiten beschouwing gelaten.

2 De opbouw en kenmerken van Blockchaintechnologie

Blockchaintechnologie kan alleen voor procesoptimalisatie zorgen wanneer deze zich positief onderscheidt in risicomitigatie ten opzichte van de traditionele IT-oplossing. Om de onderzoeksvraag te kunnen beantwoorden moeten we dus eerst kijken op welke kenmerken Blockchain zich onderscheidt en vervolgens wat die kenmerken kunnen betekenen voor een verbeterde efficiëntie in het proces.

2.1 Ontstaansgeschiedenis en werking

Al enige decennia wordt geprobeerd een digitaal betaalsysteem te bedenken dat een vertrouwde intermediair overbodig maakt. Dit is niet gelukt totdat in 2008 de Blockchain-technologie werd geïntroduceerd, onder het alias Satoshi Nakamoto (Nakamoto, S. 2008) met de Bitcoin. Het grote verschil ten opzichte van de eerdere protocollen is, dat de handtekening van een centrale server of vertrouwde intermediair hier vervangen is door consensus binnen een gedistribueerd netwerk, gebaseerd op een *proof of work* (Back et al, 2014). Het voordeel hiervan is dat het gehele netwerk nu de beslissing maakt, puur gebaseerd op een protocol en het verder geen belang heeft bij het manipuleren van de transactie. Voorwaarde is uiteraard wel dat het protocol betrouwbaar is en dat het netwerk integer is. In onderstaand figuur is de huidige situatie vs. de nieuwe situatie weergegeven.

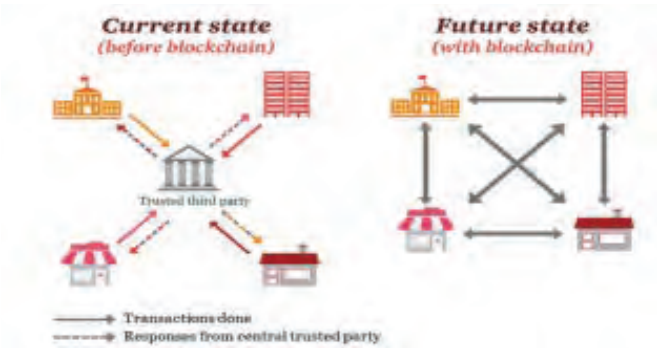


Fig.4 Het vervangen van de vertrouwde intermediair bij transacties gevisualiseerd (PWC)

De netwerkconsensus, in combinatie met de sterke encryptie, hebben als bijkomend voordeel dat de Blockchain ook goed gebruikt kan worden voor het onveranderbaar chronologisch vastleggen van andere assets, zoals persoonlijke gegevens of eigendomsbewijzen. Dat kan leiden tot meer informationele zelfbeschikking en/of betere vastlegging van de loggegevens van producten waarmee een supplychain transparanter gemaakt kan worden. Kortom, een systeem dat in meerdere opzichten in betrouwbaarheid en transparantie voorziet, daarom ook wel “trust machine” (The Economist, 2015) genoemd.

2.2 Opbouw van het Blockchainsysteem en kenmerken t.o.v. traditionele IT

Zoals in de introductie reeds genoemd is Blockchaintechnologie een combinatie van bestaande technologieën en fenomenen zoals mathematische cryptografie, (open source) software, autonome computer netwerken en, bij publieke netwerken, van incentive mechanismen. Dit maakt het een autonoom systeem dat in principe bestaat uit drie technologische dimensies, (Mougayar, 2016) ofwel lagen. De eerste twee lagen vormen de technische laag en bestaan uit het netwerk en de Blockchain. Het netwerk is opgebouwd uit nodes waarover kopieën van de Blockchain gedistribueerd zijn, die met elkaar in verbinding staan. De tweede laag bestaat uit de blockchainsoftware in de vorm van (protocol)software met een cryptografische component en de database met de versleutelde transactiedata. Via de software kunnen smart contracts gecreëerd worden waarmee businesslogic tussen verschillende netwerknodes gedistribueerd kan worden. Deze tweede laag is geïnstalleerd op alle nodes. De laatste laag betreft de functionele laag die bestaat uit

applicaties met functionaliteit. Die zijn nodig om deelnemers van de toepassing gebruik te kunnen laten maken. Deze laag kan geïntegreerd zijn of separaat via een interface aan de Blockchain gekoppeld. Dit laatste kan via een platform met applicaties (n-tier oplossing).

Deze combinatie van lagen zorgt er nu dus voor dat in een vertrouwde omgeving transacties uitgevoerd en vastgelegd kunnen worden. Een belangrijk aspect van de lagen is dat voor elke laag geldt dat deze uit meerdere varianten kan bestaan, en dat elke variant weer varieert op bepaalde kenmerken. Per laag is bekeken hoe deze opgebouwd is, wat in de literatuur de onderscheidende kenmerken zijn, en hoe deze zich per variant verhouden tot de traditionele IT. Belangrijke kenmerken zijn onder andere *Governance, Schaalbaarheid, Interoperabiliteit, Mate van (automatiseren van) vertrouwen* en *Accessmanagement*. De kenmerken zijn in drie categorieën ten opzichte van traditionele IT onder te verdelen, *Onbetwistbaar voordeel (+)*, *Onbetwistbaar nadeel (-)* en *Aandachtspunt (+/-)*. In onderstaand figuur zijn de lagen en hun onderlinge afhankelijkheden weergegeven.

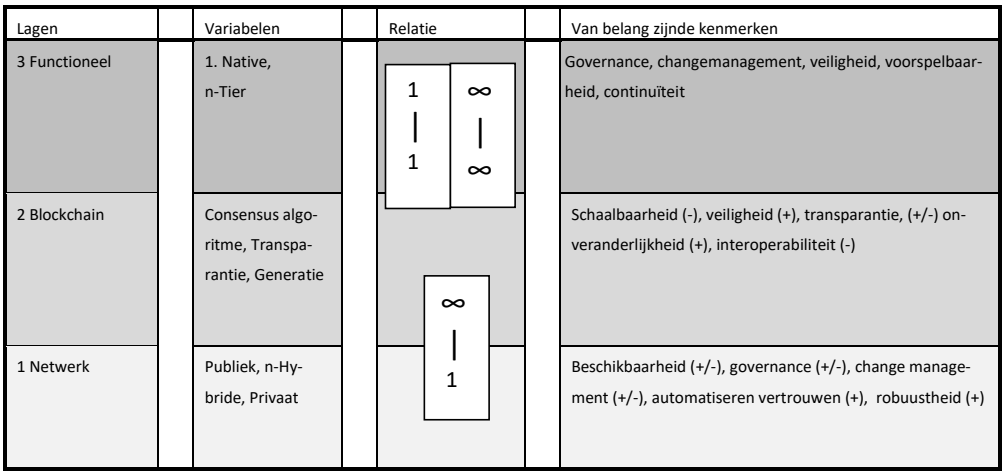


Fig.5 Opzet Blockchainsystemen met lagen, onderlinge afhankelijkheden per variabele en kenmerken.

3 Mogelijkheden tot procesoptimalisatie met blockchaintechnologie

Nu de opzet van de Blockchain bekend is, wordt dieper ingegaan op wat optimalisatie inhoudt. In de theorie wordt optimalisatie (o.a.) gedefinieerd door hogere efficiëntie en effectiviteit door continue aanpassing van het proces, binnen de randvoorwaarden (o.a. ITIL). De invulling hiervan wordt in dit onderzoek uitgedrukt in de bevordering van efficiëntie door de reductie van arbeidsintensieve beheersmaatregelen. Reductie kan plaatsvinden door het laten vervallen of automatiseren van beheersmaatregelen met behoud van randvoorwaardelijke risicomitigatie.

Uit het vorige hoofdstuk kon opgemaakt worden dat blockchaintechnologie kenmerken kent waarin zij verschilt ten opzichte van traditionele IT. Dit kunnen voordelen, nadelen en aandachtspunten zijn. Daarnaast zijn meerdere soorten blockchainoplossingen mogelijk, waarmee gevarieerd kan worden op de eerdergenoemde kenmerken. Omdat binnen een oplossing een hoge waarde van het ene kenmerk een hoge waarde van een ander kenmerk soms uitsluit, is er dus niet één generieke ideale oplossing mogelijk voor alle soorten processen. Daarom zal steeds een afweging gemaakt moeten worden, die leidt tot de blockchainoplossing die het beste aansluit bij de eisen en wensen van het betreffende proces. Dit is een belangrijke stap om te komen tot optimalisatie, maar niet de enige. Voorafgaand moet bijvoorbeeld nog getoetst worden of een proces überhaupt wel geschikt is om Blockchain toegevoegde waarde te laten hebben, of

dat een traditionele IT-oplossing volstaat. Dit betekent dat als allereerste stap de opzet van het proces in kaart gebracht moet worden, de zogenaamde IST-situatie. Nadat dit gebeurd is kan de geschiktheid van het proces voor Blockchain bepaald worden. Een belangrijk aspect hierbij is de score op de blockchainkenmerken door een procesdeskundige, dit gebeurt in stap 3 waarna in stap 4 de best passende blockchainoplossing uit de markt gekozen kan worden. Nu de gekozen blockchain bekend is kan een SOLL-situatie bepaald worden, door te kijken welke beheersmaatregelen binnen het proces ondervangen kunnen worden, of extra noodzakelijk zijn, en kan uiteindelijk in stap 6 optimalisatie vastgesteld worden.

Bovenstaande procesbeschrijving heeft geleid tot een stappenplan waarmee de aansluiting tussen de blockchain en het proces zo optimaal mogelijk gecreëerd kan worden, deze staan weergegeven in onderstaande tabel.

Nr.	Stap	Toelichting
1	*IST*-situatie bepalen	Aan de hand van scopeafbakening, de norm en een risico-analyse de interne beheersomgeving in kaart brengen, uitmondend in een procesreferentiekader.
2	Proces toetsen aan Blockchain-randvoorwaarden	Uit de theorie zijn 5 randvoorwaarden naar voren gekomen waaraan een proces vooraf moet voldoen wil het in aanmerking komen voor Blockchain.
3	Proces scoren op Blockchain-kenmerken	Het proces door een procesdeskundige op de kenmerken laten scoren en zo een profiel creëren waar een Blockchainoplossing op geselecteerd kan worden.
4	Passende Blockchain-oplossing kiezen	Bepalen welke Blockchainoplossing het beste past bij het procesprofiel.
5	*SOLL*-situatie bepalen	Aan de hand van de gekozen Blockchainoplossing bekijken welke risico's en daarmee beheersmaatregelen door Blockchain ondervangen worden en welke beheersmaatregelen eventueel extra nodig zijn.
6	Optimalisatie vaststellen	Optimalisatie kwalitatief uit te drukken in het saldo van arbeidsintensieve beheersmaatregelen.

Tabel 1 Optimalisatiemodel

4 Casestudy: IST-situatie Meldingenproces

In de vorige hoofdstukken is aan de hand van theoretisch onderzoek een optimalisatiemodel bepaald voor de toepassing van Blockchaintechnologie op een proces. In de komende hoofdstukken 4 en 5 wordt het model aan de hand van een casestudy doorlopen, zodat het model gevalideerd kan worden in de praktijk.

Om aan stap 1 van het optimalisatiemodel te voldoen is het procesreferentiekader van het betreffende casestudyproces inzichtelijk gemaakt. Het casestudyproces betreft het *meldingenproces* van het ILT, en is onderdeel van het proces Internationaal afvaltransport en –verwerking. Dit laatste proces kent als kernrisico *Onrechtmatige afvalverwerking*. Om dit risico te minimaliseren zijn er, via de norm EVOA, meerdere beheersmaatregelen ingesteld. Eén van die beheersmaatregelen is dus het *meldingenproces* waarbij op meerdere tijdstippen meldingen gedaan moeten worden over het afvaltransport en de verwerking. Hierdoor kunnen de randvoorwaarden en status van het transport goed gemonitord en gecontroleerd worden. Er zijn meerdere partijen betrokken, en het proces kent een sterke administratieve component omdat alle partijen bij elke controle (= informatiestatuswijziging) snel een gelijkwaardig informatieniveau moeten hebben. Daarbij moet elke informatiestatus direct aan een partij-identiteit te koppelen zijn. Dit is een zeer arbeidsintensief proces omdat bij elke statuswijziging alle relevante documenten getekend en naar alle relevante partijen rondgestuurd moeten worden. Belangrijke geconstateerde proceskenmerken hierbij zijn *authenticatie*, *administratie, eenduidigheid en tijdigheid*.
In onderstaande tabel is het huidige kader (IST-situatie) van het meldingenproces met actoren weergegeven.

Niv.	Processtappen			Actoren					
	Code	Omschrijving	Doel	ILT	Verzender	Externe consultant	Transport	Handhaving	Ontvanger/ verwerker
1	A1	Voornemen tot ontdoening	Initiatie proces						
2	A1-1	Melding met kenmerken afvaltransport	ILT/Regulator in staat stellen te monitoren/controleren	I	A,R	I			
2	A1-2	Controle melding ILT en akkoord	Voldoet melding aan licentievoorwaarden	A,R	I	I		I	
2	A1-3	Controle melding door regulator land van herkomst / bestemming en akkoord	Voldoet melding aan licentievoorwaarden	I	I	A,R		I	
1	A2	Transport							
2	A2-1	Voornemen tot transport	Toezichthouders informeren over status en in staat stellen te controleren.	I	A,R	I	I	I	I
2	A2-2	Risico gestuurde inspectie door handhaving	Controle vooraf/tijdens transport op rechtmatigheid	I		I		A,R	
1	A3	Ontvangst/ verwerken							
2	A3-1	Ontvangstmelding afval	Inzicht ILT in locatie afval	I					A,R
2	A3-2	Melding verwerking afval	Inzicht ILT in status afval	I					A,R
2	A3-3	Risico gestuurde inspectie door overige handhaving	Controle vooraf/tijdens verwerking op rechtmatigheid	I		I		A,R	
1	A4	Afronding	Afsluiten proces						

Tabel 2 Procesreferentiekader Meldingenproces (R=Responsible, A=Accountable, C=Consulted, I=Informed)

5 Casestudy: Soll-situatie Meldingenproces

In het vorige hoofdstuk is de IST-situatie inzichtelijk gemaakt, waarmee stap 1 van het optimalisatiemodel genomen is. In het komende hoofdstuk worden de stappen 2 t/m 6 doorlopen, en wordt bekeken hoe blockchaintechnologie voor dit proces kan bijdragen aan optimalisatie.

5.1 Keuze passende blockchainoplossing

Allereerst is de fit tussen Blockchain en proces bepaald, door stap 2 t/m 4 te doorlopen. Concreet betekent dit eerst via stap 2 het proces toetsen aan - voor blockchaintechnologie randvoorwaardelijke - basiseigenschappen, zoals meerdere partijen die gegevens moeten uitwisselen en die elkaar niet vertrouwen. Het proces kent deze eigenschappen waarmee aangetoond is dat Blockchain dus van toegevoegde waarde kan zijn. Hierna volgden stappen 3 en 4 waarmee aan de hand van de waardering van de blockchainkenmerken op dit specifieke proces de juiste blockchainoplossing gekozen kon worden. Vanwege de vereiste afscherming van gegevens en de benodigde transactiesnelheid (prestatie/schaalbaarheid) is een hybride (private) vorm met een consensus-algoritme van minimaal (P)BFT of sneller benodigd. Omdat ook enige mate van businesslogic nodig is, is een tweede generatie Blockchain met de mogelijkheid tot het bouwen van Smartcontracts essentieel. Voor de functionele laag is een oplossing via een platform met een applicatielaag het meest voor de hand liggend, gezien de benodigde functionaliteit op maat.

Lagen		Voorgestelde variabele
Functioneel		n-Tier
Blockchain		PBFT of sneller; 2e gen.;
Netwerk		Hybride

Tabel 3 Voorgestelde blockchainoplossing

Aanvullende constateringen voor het optimalisatiemodel waren dat bepaalde waardes van blockchainkenmerken die door het proces als eis gewaardeerd zijn, al snel de randvoorwaarden van de Blockchainoplossing bepalen. En dat als er twee conflicterende eisen zijn er wellicht geen mogelijke Blockchainoplossing voorhanden is. Dat laatste was in deze case overigens niet het geval.

5.2 Impact op arbeidsintensieve beheersmaatregelen op applicatieniveau

Na de best passende blockchainoplossing gekozen te hebben zijn de stappen 5 en 6 gevolgd en is gekeken naar de processtappen en beheersmaatregelen en wat de gekozen Blockchainoplossing daar aan optimalisatie in kan betekenen. Zoals in hoofdstuk 4 reeds geconstateerd is, vormt identificatie gekoppeld aan informatiestatus een belangrijk onderdeel in het proces. Dat aspect zorgt voor veel extra noodzakelijke manuele en computerafhankelijke maatregelen. Op dit vlak is dan ook gekeken wat Blockchain concreet kan betekenen aan reductie. Blockchain is in staat om via accesmanagement in combinatie met versleuteling de identiteit rechtstreeks in de database aan informatie te koppelen en onveranderlijk te maken, waarmee de meeste van deze maatregelen ondervangen worden en kunnen vervallen. Daarbij wordt de momenteel gefragmenteerde administratie en werkwijze samengevoegd naar een eenduidige administratie en werkwijze wat efficiëntie in de hand werkt. Zie figuur 6.

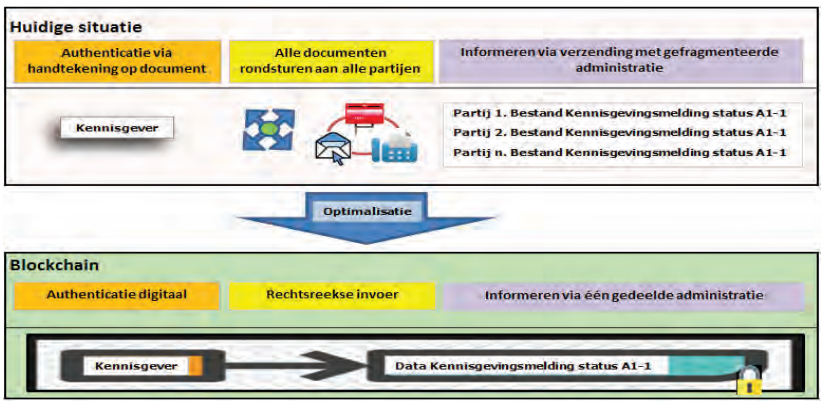


Fig.6 Voorbeeld processtap A1-1, waarbij de arbeidsintensieve maatregel ter informeren sterk vereenvoudigd wordt.

Tijdens het onderzoek is ook nog gekeken naar de mogelijkheid om het fysieke onderdeel, namelijk het primaire proces afvaltransport en –verwerking, in het systeem te includeren. Het voordeel hiervan is dat er dan geen centraliteit in het systeem meer nodig is wat tot verdere reductie in beheersmaatregelen kan leiden. Echter het asset waar het hier om gaat, het afval, is een fysiek asset dat met de huidige technologie nog moeilijk te koppelen is. Dit deel is daarom niet verder uitgewerkt. Hierdoor blijven beheersmaatregelen als transportmeldingen en risicogestuurde controles op de weg nodig, en blijft daarmee ook een mate van toezicht en noodzakelijk.

De scope voor de procesoptimalisatie is gericht op de risicomitigatie op het applicatielevel, die het gevolg is van de directe toegevoegde waarde van de Blockchain. Daarbinnen zijn geen extra maatregelen geconstateerd.
Binnen de ITGC-aandachtsgebieden zijn echter enkele interessante aspecten opgevallen die buiten de scope vallen, maar wel vermeldenswaardig zijn omdat ze voor extra beheersmaatregelen (kunnen) zorgen. Zo is binnen Accesmanagement het keymanagement veel belangrijker geworden omdat er een veilige omgeving gecreëerd is, waar juiste identificatie en authenticatie van essentieel belang zijn. Verder geldt dat werken met een Blockchain inherent staat aan het werken in één autonoom systeem met meerdere partijen. Dit heeft tot gevolg dat per ITGC-aandachtsgebied het binnen de deelnemende partijen hoogst scorende risicoprofiel leidend wordt voor het gehele systeem. Dit kan dus consequenties hebben voor de ITGC-aandachtsgebieden van de overige partijen. Verdere analyse daarop valt echter buiten de onderzoekscope.

5.3 Geactualiseerd proceskader na Blockchaintoepassing

Onderstaand kader is het nieuwe kader aan maatregelen, nadat de meest optimale blockchainoplossing is toegepast. Dit nieuwe referentiekader is de grondslag voor de SOLL-situatie van het casestudyproces. In onderstaand kader is te zien dat er op dit niveau geen stappen zijn gewijzigd of vervallen. Concrete reductie heeft echter wel een niveau lager binnen de hier weergegeven stappen plaatsgevonden en is in de toelichting beschreven. Zoals te zien is valt er binnen bijna alle stappen optimalisatie te behalen. De schaal van optimalisatie loopt van 0 t/m 2, waarbij 0 = geen/weinig, 1 = optimalisatie, 2 = sterke optimalisatie.

Niv	Processtappen			Actoren						Optimalisatie na toepassen Blockchaintechnologie (stap 6)	
	Code	Omschrijving	Doel	ILT	Verzender	Externe re-	Transport	Handhaving	Ontvanger/ verwerker	Mate van opt.	Toelichting
1	A1	Voornemen tot ontdoening	Initiatie proces							2	Kan sterk geoptimaliseerd worden
2	A1-1	Melding met kenmerken afvaltransport	ILT/Regulator in staat stellen te monitoren/controleren	I	A,R	I				2	Fysiek formulier invullen, ondertekenen en rondsturen wordt vervangen door rechtstreekse invoer in 1 centrale administratie met identiteit-koppeling door elektronische authenticatie.
2	A1-2	Controle melding ILT en akkoord	Voldoet melding aan licentievoorwaarden	A,R	I	I		I		2	Fysiek formulier controleren, ondertekenen en rondsturen wordt vervangen door: ingevoerde gegevens controleren en afvinken, netwerkorganisatie wordt automatisch geïnformeerd.
2	A1-3	Controle melding door regulator land van herkomst / bestemming en akkoord	Voldoet melding aan licentievoorwaarden	I	I	A,R		I		2	
1	A2	Transport								1	Kan geoptimaliseerd worden
2	A2-1	Voornemen tot transport	Toezichthouders informeren over status en in staat stellen te controleren.	I	A,R	I	I	I	I	2	Fysiek formulier invullen, ondertekenen en rondsturen wordt vervangen door rechtstreekse invoer in 1 centrale administratie met identiteit-koppeling door elektronische authenticatie.
2	A2-2	Risico gestuurde inspectie door handhaving	Controle vooraf/tijdens transport op rechtmatigheid	I		I		A,R		0	Moet blijven bestaan, enige verbetering is de hogere betrouwbaarheid van de gege-

											vens voor de risicogestuurde controles.
1	A3	Ontvangst/ verwerken								2	Kan sterk geoptimaliseerd worden
2	A3-1	Ontvangstmelding afval	Inzicht ILT in locatie afval	I					A,R	2	Fysiek formulier invullen, ondertekenen en rondsturen wordt vervangen door rechtstreekse invoer in 1 centrale administratie met identiteit-koppeling door elektronische authenticatie.
2	A3-2	Melding verwerking afval	Inzicht ILT in status afval	I					A,R	2	
2	A3-3	Risico gestuurde inspectie door overige handhaving	Controle vooraf/tijdens verwerking op rechtmatigheid	I		I		A,R		0	Moet blijven bestaan, enige verbetering is de hogere betrouwbaarheid van de gegevens voor de risicogestuurde controles.
1	A4	Afronding	Afsluiten proces								

Tabel 4 Geactualiseerd procesreferentiekader

5.4 Evaluatie optimalisatiemodel

Het optimalisatiemodel zelf is goed toepasbaar gebleken. Duidelijk werd welke blockchainvorm mogelijk was en welke beheersmaatregelen konden veranderen. Naar aanleiding van de praktijktoetsing kan het optimalisatiemodel tevens iets verder genuanceerd worden (rood onderstreept):

Nr.	Stap	Toelichting
1	*IST*-situatie proces bepalen	Aan de hand van scopeafbakening, de norm en een risico-analyse de interne beheersomgeving in kaart brengen, uitmondend in een procesreferentiekader.
2	Proces toetsen aan Blockchain-randvoorwaarden	Uit de theorie zijn 5 randvoorwaarden naar voren gekomen waaraan een proces vooraf moet voldoen wil het in aanmerking komen voor Blockchain.
3	Proces scoren op Blockchain-kenmerken	Specifiek voor dit proces een profiel creëren waar later een Blockchainoplossing op geselecteerd kan worden. *Als eis gewaardeerde kenmerkwaarden vormen de randvoorwaarden van de blockchainoplossing. Als de kenmerkwaarde van twee of meer eisen conflicterend zijn, kan Blockchain wellicht niet de juiste oplossing zijn, en verdient het aanbeveling naar alternatieven te kijken.*
4	Passende Blockchain-oplossing kiezen	Bepalen welke Blockchainoplossing het beste past bij het procesprofiel.

5	*SOLL*-situatie proces bepalen	Aan de hand van de gekozen Blockchainoplossing bekijken welke risico's en daarmee beheersmaatregelen door Blockchain ondervangen worden en welke beheersmaatregelen eventueel extra nodig zijn. *De ITGC's van de partij met de hoogste eisen worden vigerend voor het hele systeem, dit kan zorgen voor extra maatregelen ten opzichte van de IST-situatie van de overige partijen.*
6	Optimalisatie vaststellen	Optimalisatie kwalitatief uit te drukken in het saldo van arbeidsintensieve beheersmaatregelen.

Tabel 5 Optimalisatiemodel geactualiseerd na praktijktoets

6 Conclusie

De hoofdvraag van het onderzoek luidde:
In hoeverre kan een hoog compliant proces geoptimaliseerd worden door toepassing van blockchaintechnologie?

Om optimalisatie te bereiken door Blockchain moet er positief onderscheid zijn ten opzichte van de traditionele IT-oplossingen. Om dat inzichtelijk te krijgen is geanalyseerd hoe Blockchaintechnologie in elkaar zit, om zo de voordelen zo effectief mogelijk te kunnen benutten. Dit heeft geleid tot inzicht in de opbouw die gelaagd is en per laag uit variabelen bestaat. Deze variabelen kennen weer meerdere kenmerken waarin Blockchain zich onderscheidt ten opzicht van traditionele IT. Dit zijn naast positieve kenmerken echter ook negatieve kenmerken en aandachtspunten. Een belangrijke constatering hierbij is dat de waarde van de kenmerken *verschillen* per variabele. Omdat elke proces zijn eigen belangrijke kenmerken heeft bestaat er dus niet één generieke Blockchainoplossing die alle processen optimaal kan bedienen. Er moet daarom per proces een zo *optimaal mogelijke* keuze van variabelen gemaakt worden om te komen tot een passende blockchainoplossing. Daarbij dient het proces aan enkele randvoorwaarden te voldoen om Blockchain überhaupt van toegevoegde waarde te laten zijn.

Om een zo optimaal mogelijke fit tussen blockchaintechnologie en het betreffende proces te realiseren, is een optimalisatiemodel ontwikkeld. Dit is vervolgens toegepast op een usecase zodat het in de praktijk gevalideerd kon worden. Het model bleek goed te werken. Er zijn geen tekortkomingen geconstateerd en er is voldoende diepgang behaald om optimalisatie als gevolg van reductie van beheersmaatregelen te kunnen bepalen. Er hoeven dus geen stappen toegevoegd of verwijderd te worden, wel zijn enkele nuances binnen de stappen aangebracht.

Het optimalisatiemodel is vervolgens toegepast op een usecase. Deze usecase, het zogenaamde *Meldingenproces*, is een beheersmaatregel die noodzakelijk is om het risico van milieu- en gezondheidsschade door illegale afvalverwerking te mitigeren. Vanwege de hoge mate van compliance wordt er momenteel veel administratie rondgepompt. Gebleken is dat Blockchain hier een sterke optimaliserende rol in kan spelen, door de mogelijkheid tot directe koppeling van identiteit aan informatie en het samenvoegen van de administraties in één database. Tevens is geconstateerd dat Blockchain niet in staat is de gehele beheersmaatregel te ondervangen omdat dan tevens het fysieke asset, het afval, onlosmakelijk verbonden zou moeten worden aan de Blockchain. Dat is op dit moment nog onvoldoende mogelijk. Daardoor blijft controle en toezicht nodig op het daadwerkelijk transport en verwerking, wat leidt tot een Blockchain waarin nog steeds centraliteit noodzakelijk is.

Concreet is het antwoord op de hoofdvraag dus dat procesoptimalisatie weldegelijk mogelijk is vanwege de risico's die Blockchaintechnologie kan ondervangen, waardoor beheersmaatregelen geschrapt kunnen

worden. Wel dienen meerdere stappen doorlopen te worden zodat de juiste fit tussen de te kiezen Blockchainvorm en het proces gecreëerd kan worden.

7 Aandachtspunten en nuancering

7.1 Aandachtspunten

Voor de procesoptimalisatie door Blockchaintoepassing is in dit onderzoek, gezien de beperkte mogelijkheden, alleen naar de directe besparingen op applicatielevel gekeken. Echter om optimalisatie te bewerkstelligen is naast een efficiënter proces onder andere een goed functionerende IT-organisatie met ITGC's op de achtergrond van essentieel belang. Deze maatregelen zijn wel bekeken in het theoretisch onderzoek en op dit gebied zijn drie aandachtspunten geconstateerd:

1. Risicoprofielen veranderen in publieke Blockchains

Binnen het publieke blockchainnetwerk opereren allerlei groepen met verschillende belangen. Om (noodzakelijke) veranderingen doorgevoerd te krijgen is netwerkconsensus nodig. Het risico bestaat dus dat het belang van een betreffende netwerkorganisatie niet doorgevoerd wordt, of dat er een ander ongewenst belang wel doorgevoerd wordt. Dit is vooral een risico voor changemanagement in de technische laag. Hardforks en ook hapering in de continuïteit van de werking van de Blockchain kunnen het gevolg zijn. Het verdient dan ook aanbeveling hier extra maatregelen voor te nemen.

2. Verhoogde risico's aan de rand van het systeem

Omdat er met de Blockchain een veilig systeem gecreëerd is, dient alle informatie die van buiten naar binnen gaat, extra gecontroleerd te worden om data-integriteit te waarborgen. Dit betekent extra maatregelen op de aandachtsgebieden *Accesmanagement* en *Veiligheid* tussen separate lagen en systemen. Geconcludeerd kan worden dat er beheersmaatregelen zijn verschoven van intern in het proces naar de randen van de systeemscope.

3. Het hoogst scorende ITGC-risicoprofiel binnen de netwerkorganisatie wordt leidend

Een belangrijke andere constatering is dat vanwege het feit dat Blockchain inherent staat aan het werken in één autonoom systeem, dit betekent dat per ITGC-aandachtsgebied het hoogst scorende risicoprofiel van alle partijen binnen de netwerkorganisatie leidend wordt voor het systeem. Aanbeveling is hier rekening mee te houden bij de proceswaardering van de kenmerken door de verschillende partijen.

7.2 Nuancering

De voordelen genoemd in de conclusie blijven wel case gerelateerd en er moet goed over de toepassing ervan nagedacht worden. Een compleet geautomatiseerd en vastliggend systeem kent voordelen maar ook nadelen. Een nadeel is dat voor uitzonderingen, onvoorziene gebeurtenissen, of het redelijkheid- en billijkheidsprincipe weinig plaats is. Ook blijft data-integriteit door onjuiste invoer (door fouten of (identiteits)fraude) een niet te onderschatten risico. Daarom zal de Blockchain naar mijn idee nooit de gehele informatieverwerking overnemen, maar zal die gericht en effectief toegepast moeten worden binnen het grotere geheel van dataverwerking.

Managing the risks of using end user computing solutions

Jasper Kroeger

In 2011, Jasper Kroeger graduated with a MSc Information Management degree at Tilburg University. This was the start of his career in the field of IT, Information Risk Management, and IT audit. After his graduation, Jasper started at PwC Amsterdam as IT Auditor.
His most important motivator to become an IT auditor was and is to thoroughly understand the challenges and points of improvement of processes, projects, and organizations in general. Supporting organizations to improve their governance and processes on strategic, tactical, and operational level is something that strongly satisfies him.
In 2018, Jasper finished the Postgraduate IT Audit, Compliance and Advisory program at the VU Amsterdam. A summary of the conducted research to finish the program is included below.
Currently, Jasper is working as Manager Information Risk at LeasePlan. In this job, he is able to apply his knowledge and experience to adequately secure the information of LeasePlan physically and digitally.

1 Introduction

End user computing (EUC) is not a new phenomenon. For years, organizations have been struggling with the shortcomings of applications. This can for example be a shortcoming in reporting functionalities or a gap between the implemented and desired functionalities. Organizational departments and end users are very creative in creating solutions for these gaps.

Spreadsheets are a commonly used solution to perform calculations or to make data/ information presentable for stakeholders. In the case of a gap between desired and implemented functionalities in business software, spreadsheets can be used to process (manipulate) data/ information from an application followed by importing the output back to the application. These spreadsheets or comparable solutions are called EUC solutions.

At every level (strategic, tactical, and operational) organizations heavily lean on the strengths and flexibility of EUC solutions. However, using and depending on EUC solutions exposes organizations to a certain level of risk. The reliability of spreadsheets is difficult to manage. This is a challenge for the internal organization as well as for external auditors like Accountants/ IT Auditors.

Many studies have already been performed on EUC in general and more specific on EUC solution risk management. However, a holistic and practical approach for developing, implementing, and maintaining an EUC risk management system was not yet available.

1.1 Research questions

By means of this research, we investigate how organizations can effectively manage the risks of using EUC solutions. To perform this research, we defined a main research question and three sub research questions.

1.1.1 Main research question

How can organizations implement an approach to effectively manage the risks of using EUC solutions and which recommendations can be given?

1.1.2 Sub research questions

- *Theoretical research*
    1. What are EUC solutions, why do they exist, and which controls are generally used to mitigate the risks of using them?

- *Analytical research*
    2. Which controls do organizations implement in practice to manage the risks of using EUC solutions and what does a practical EUC risk management approach look like?

- *Synthesis*
    3. Which recommendations can be given to implement an approach to manage the risks of using EUC solutions?

2 Theoretical research

In this chapter, we investigate what EUC solutions are and which controls are generally used to mitigate the risks of using them. Based on the book 'A brief History of Computing' written by O'Regan, G. (2012), we start with looking back to the past to investigate the rise of decentralized computing followed by the evolution of EUC until now. After that, we define the term EUC solution. The next step is to research why organizations use EUC solutions and to what risks they are exposed when using them. We also have a closer look on the vision of regulators on using EUC solutions. The last two paragraphs describe why organizations

should implement an EUC risk management approach and which controls are generally used as mitigating measures.

2.1 What are EUC solutions?

Different appellatives, definitions, and abbreviations are used in literature and practice to describe and define the solutions used by organizations to compensate the shortcomings of applications. However, all descriptions have in common that for different reasons (refer to paragraph 2.2), end users choose to develop their own solutions to meet their needs.

2.1.1 The rise of decentralized computing

The way we use computers changed significantly during the past 70 years. Nowadays, at every level in organizations, many workers interact with computers to accomplish their work. In private live, almost everybody has computers in their homes. We should also not forget the mobile devices we use every day. However, this has not always been the case. When computers were first used in business, most people did not have computers on their office desks, or in private live. In short, the evolution of information technology changed from centralized mainframe computers, to ubiquitous (anytime and anywhere) computing.

It started in the 1950s and 1960s. During this period, computer systems in business and government were highly centralized. These systems are called mainframe computers. Mainframe computers are large, powerful computer systems that process high volumes of transactions, store databases with millions or billions of records, and often serve as the hub of a corporate network. Only IT professionals had direct access to these computers and had the ability and access to develop software, enter information, perform calculations, and produce reports. Employees in other departments had to request services from the IT professionals and then wait for the results. Because the number of available mainframe computers was very limited, data for input had to be delivered physically (punched cards of paper/ magnetic tape) to the central system location. Output (payroll checks or printed reports) had to be delivered back to the department where it was used or distributed.

During the 1970s, the use of computers gradually became decentralized in many organizations. In this period, terminals became common. A terminal consists of a keyboard and a display that are connected to a mainframe computer. These terminals did not have process or storage capabilities. Although the data was still stored and processed centrally in the mainframe computer, employees were able to run programs and input and retrieve data themselves without leaving their desks. However, mainly because of the high costs, organizations were not able to provide a terminal to each employee. Interesting is the fact that the mainframe IT professionals were not so happy with terminals. They often expressed the concern that errors and mistakes made by employees in other departments could offset any productivity gains from terminal access to the mainframe.

With transaction processing systems to handle common manual processing tasks (such as Payroll, Inventory management, and Finance), managers began to think of new ways to use computer technology. However, IT professional staffs were not able to grow fast enough to meet the increasing demands. This is one of the developments that empowered the widespread transition to decentralized computing.

Since the 1980s and 1990s many employees in various industries began to use computers directly. An important reason for this shift was a huge drop in the costs to provide computer power directly to employees. The first personal computers appeared in some organizations during the early 1980s. The development of inexpensive software contributed to the rapid expansion of personal computers. Software packages such as Visi-Calc (spreadsheet), WordStar (word processor), Lotus-1-2-3 (spreadsheet), and dBASE (database) meant that organizations could afford not only the hardware, but also the software that would make their employees more productive. In addition to inexpensive productivity software, industry-standard operating systems such as MS-DOS, MacOS, and Windows, contributed to the rise of decentralized computing.

In the late 1990s and 2000s, the era of distributed and network computing arose. Both centralized mainframe computing and decentralized computing share a common goal: help employees be more productive.

However, the way people interact with computers has changed dramatically. Widespread use of computer networks and the use of Internet as a communication tool increased the use of electronic business and business-to-business transactions and will continue to have a significant impact on businesses and home computer users.

2.1.2 The evolution of EUC solutions

Mainframe systems and its underlying software were developed and used to gain efficiency by automating repeating tasks. The use of software to replace manual tasks was extremely profitable for organizations. In the early days of office automation, accounting software was one of the most popular business software tools.

After this period, when computer power became available for a large number of employees, other software was developed. The most noticeable, widespread change in business software was the word processor, followed by mathematical spreadsheet programs. Also, more and more software was developed to automate other business processes. This resulted in the rise of Enterprise Resource (ERP) software, supporting the whole chain of business processes.

The described developments caused a significant growth in demand for software functionalities. IT departments were not able to meet all these demands. The lack of available functionalities and the long lead times of IT departments were incentives for employees to take the matters into one's own hands. This increased the amount of computing being done by end users. Other motivators for end users to choose for EUC are:

- End users have more control over system development and use.
- Procedures of the IT department are not appropriate for small applications.
- The IT department is not perceived as being concerned about users' needs.
- End users are eager to learn about computing.
- End users gain more flexibility.

Also, the do-it-yourself mentality is prevalent in society today, and EUC fits well with this mindset. EUC gives the user control over building solutions because explaining subject areas or technical requirements to an IT specialist is not required. Further, the end user controls the time schedule of the development, which generally results in a quicker usable solution. The end user employs his own resources in developing and therefore does not have to wait for funding and scheduling the project through an IT department's budgetary process.

Spreadsheets are the most common data analysis and manipulation tools used by end users in organizations. Spreadsheets are often used as tools for modelling information relevant for management decision-making. For instance, pivot tables are often used for multidimensional analysis since they provide rollup, drill-down, and slice-and-dice functionality.

2.1.3 Defining EUC solutions

As stated in the introduction, a high variety of definitions are used to describe the phenomenon of EUC. We selected five definitions that are published between 1986 and 2011 (refer to table 2.1).

Name (abbreviation)	Definition	Author(s)
User Developed Application (UDA)	UDAs are applications that are developed by end users, usually in a noncontrolled IT environment.	Belino, C.A., Ochab, D., and Rowland, J.S. (2010)
End User Computing (EUC)	EUC is the use and/or development of information systems by the principal users of the systems' outputs or by their staffs.	Leitheiser, R.R., and Wetherbe, J.C. (1986)
End-user computing (EUC)	End-user computing had been identified as "the autonomous use of information technology by knowledge workers outside of the information systems department".	Baškarada, S. (2011)

End-user computing (EUC)	An information system developed by the users themselves rather than IT professionals to meet company operational or management information needs.	Romney, M., and Steinbart, P. (2006)
End user computing (EUC)	The adoption and use of information technology by personnel outside the information systems department to develop software applications in support of organizational tasks.	Brancheau, J., and Brown, C. (1993)

Table 2.1: EUC definitions

After analyzing these definitions, we concluded that there is one important different view on wat EUC comprises. Baškarada (2011) states that EUC is the use of computer power by knowledge workers outside the IT department. He does not mention the development of applications by the end users. The other four authors do mention that EUC is the development of software functionalities by end users. Romney and Steinbart (2006) include in their definition that EUC is used to meet company operational or management information needs. We consider this as an important addition that distinguishes this definition from the others. Therefore, we choose to use the definition of Romney and Steinbart (2006) in this thesis.

2.2 Why do organizations use EUC solutions?

In this paragraph we investigate why organizations use EUC solutions. In paragraph 2.1, we have already argued several reasons why end users choose for EUC solutions. Flexibility, control, and the availability of IT professional development hours are noted as important factors.

An interesting question is why (senior) management allows it to happen. Do they recognize the requirements of end users and permit their choice for taking the matters into one's own hands? Or does (senior) management whether consciously or not force end users to make these choices? For example, by demanding fast and ad hoc management reports, while not providing enough development hours for IT/ reporting professionals.

Organizations will continue their efforts to migrate functionality from EUC solutions into ERP packages or other more controlled business applications, but EUC solutions will not be going away anytime soon.

2.2.1 What are the main reasons for organizations to use EUC solutions?

Spreadsheets are used extensively in business, for all sorts of tasks and purposes. While other assets of companies - like software products and processes - are strongly guarded, spreadsheets are usually not structurally managed.

This lack of control contrasts the potential impact of errors, which can be widespread, as previous studies have shown. For instance, Hall (1996) interviewed 106 spreadsheet developers and found that only 7% of the spreadsheets were of low importance and that as much as 39% were of high importance. In a more recent study we found similar results (Hermans et al., 2012). However, spreadsheets are often of dubious quality, as there are no widely accepted spreadsheet design policies and they are hardly ever enforced or checked.

A survey performed by Deloitte (2009) indicates that 70% of the 2.804 companies in scope of the research rely heavily on spreadsheets for critical portions of their business processes or to complete their financial reporting.

EUC solutions continue to present both opportunities and challenges for organizations. EUC solutions allow organizations to respond quickly and effectively to dynamic market conditions. The side effect is that companies became too dependent on EUC functionalities.

EUC solutions provide a great benefit by allowing users to directly manage, control and manipulate data. Unlike SAP, Oracle, and other enterprise resource planning (ERP) applications that facilitate the automated and integrated flow of transactions and data, EUC solutions are neither ponderous nor difficult to modify. In fact, EUC solutions allow businesses and users to quickly deploy solutions in response to shifting market

and economic conditions, industry changes or evolving regulations. They can also help to overcome functionality gaps experienced in ERP systems.

Leitheiser and Wetherbe (1986) state that the use of EUC solutions has been motivated by the inability of the IT department to meet computing needs of end users and management. Therefore, end users choose to do their own computing because:

- lead times on development requests are shorter;
- end users have more control over system development and use;
- services are not available from the IT department;
- IT procedures are not appropriate for small applications;
- the IT department is not perceived as being concerned about the users' needs;
- end users want to learn about computing;
- end users gain more flexibility;
- the applications developed better meet end users' needs;
- development costs seem to be lower.

Besides the advantages for end users, Leitheiser and Wetherbe (1986) state that IT departments also benefit from the development and use of EUC solutions. First, the shortage of systems development personnel can be relieved. This allows IT management to use their human resources on larger, more technical development projects. Second, if end users know their requirements, they can implement them directly into an application. At last, system implementation becomes the responsibility of the operational departments. Their ownership of the system is therefore insured and a major stumbling block to successful system implementation is removed.

The study of Baškarada (2011) identifies ad hoc reporting as the main reason for using EUC solutions. Even though most of the transactional and business intelligence (BI) systems provide reporting functionalities, there are several reasons why they are not commonly used:

- Lack of capital expenditure (CAPEX) funding.
- The system development life cycle process is too complex.
- The time frame required for development is too long.
- Many analysts and managers often prefer to export raw data from source systems and analyze/ manipulate it in EUC solutions as required.

2.3 Risks of using EUC solutions

In the previous paragraphs, we have conducted research of what EUC solutions are and why organizations use them. Research shows that a huge amount of organizations uses EUC solutions. Auditors are having a hard time to gain comfort on these applications and the impact on financial statements and decision-making. The lack of controls around the development, use, and management of EUC solutions often leads to audit findings during the annual financial statement audit. In paragraph 2.5, we elaborate in more detail on relevant regulations that provide legislation and/ or guidelines on using EUC solutions.

To be able to understand the side effects of using EUC solutions and to develop an adequate mitigation approach, research on the risks of using EUC solutions is needed. To ensure completeness in identifying the risks, we use a software development lifecycle methodology, which describes all phases in the lifecycle of a piece of software as a basis.

Many different software development lifecycles were defined since software is developed (Ruparelia, 2010). We should be aware that a software development lifecycle is a theoretical model. In practice, the development of EUC solutions may vary in different forms. This could be considered as a risk in general. However, whether it may be formalized or not, the development of an EUC solution follows certain process steps which can be linked to a software development lifecycle.

Rapid Application Development (RAD) comes closest to the development of EUC solutions because there is high involvement of end users, prototyping is used as a mechanism, and a low degree of formalization and documentation is generally applied. Therefore, we use this methodology to identify the risks of EUC solutions during its entire lifecycle. The RAD methodology is shown in the figure below (figure 2.1).

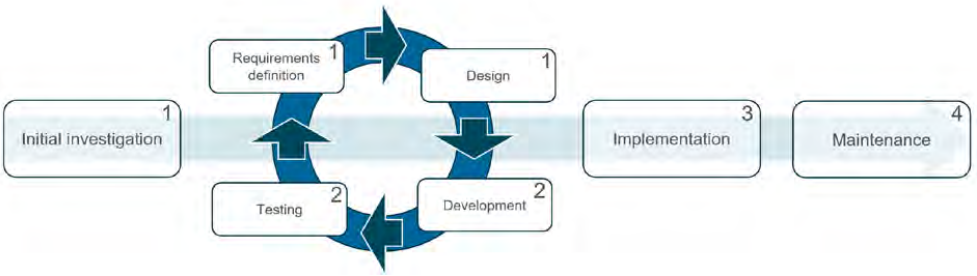


Figure 2.1: RAD methodology

There is a certain level of overlap between the different phases in the RAD methodology shown in figure 2.1. Therefore, in this thesis we combined 'initial investigation', 'requirements definition', and 'design'. We also combined 'development' and 'testing'. Combining these process steps leads to four main phases in the lifecycle of EUC solutions (refer to numbers in figure 2.1). For each phase, organizational risks regarding the usage of EUC solutions are identified and described in the following sub-paragraphs. Researching risks in the different phases of the EUC solution lifecycle helps us to define the controls needed to be able to decrease the likelihood and impact of negative effects caused by using EUC solutions.

2.3.1 Initial investigation, requirements definition, and design

In most cases, EUC solutions are developed with little or no analyst specialism involvement. End users are not data processing professionals or programmers. Rather, they are corporate planners, financial analysts, or market researchers. It has been shown in research that the quality of EUC solutions is dependent on the relevant knowledge of users and developers. However. experiments have also shown that even a substantial percentage of EUC solutions created by experienced users contain errors (Deloitte, 2009).

Under the pressure of daily activities, end-users may not spend enough time on problem definition and diagnosis. End-users are likely to proceed with solving the problem (creating a new EUC solution) without adequate problem specifications. Hence, end-users are more likely to solve the wrong problem (Alavi and Weiss, 1985). Often, end users spend an inordinate amount of time developing an application, only to find that there is existing software that already performs the task (Jenne, 1996).

The lack of initial investigation and requirements definition leads to a risk that organizations will likely waste scarce resources developing EUC solutions due to:

- duplication of applications within the same company, as individual departments create similar end-user solutions for a common problem but do not share them across departmental boundaries;
- the risks of users spending hours on designing and developing an EUC solution that an expert could have developed in a few minutes or using more efficient technology;
- the use of unusual development software that does not communicate with the company's standard platform;
- a potential risk that, by getting too involved in EUC solution development, end-users are becoming sidetracked from their primary organizational responsibilities.

2.3.2 Development and testing

The development process of EUC solutions is best characterized as incremental and evolutionary. The development process usually does not include documentation, formal validation procedures, and extensive

testing. End-users avoid documentation because they typically view it as a waste of time and an unnecessary activity. The lack of documentation leads to risks by means of (external) reviews, future modification, and a knowledge gap if the initial developer leaves the organization (Alavi and Weiss, 1985).

The segregation of duty functionalities that are built into systems developed via regular (IT) development processes does normally not exist in EUC solutions. In many cases, the developer is simultaneously sponsor, programmer, tester, and user (Deloitte, 2009). End-users are reluctant to extensively test the solutions that they develop because testing is time consuming. Besides, most users are unaware of many possibilities for errors.

The lack of a formal development and test process leads to the risk of developing EUC solutions with (unintentional) errors. Increasing the risk of errors is the problem that users tend to be overconfident in their solution development abilities (Panko, 2006). The selection of EUC solution tools can also be a source of errors. End users frequently select the tool they know best, rather than the best tool for the job. The most common example is when end users develop applications using spreadsheets, when a database tool would be better.

2.3.3 Implementation and usage

Closing the books faster and more efficiently is a very important goal for finance leaders, but departments that use spreadsheets for the process are at a considerable disadvantage. According to a study performed in 2005, 54% of companies that characterized themselves as substantial spreadsheet users take seven or more days to perform the month-end closing process.

EUC solutions are relatively fast and easy to set up, but when they are used in collaborative, repetitive enterprise processes, they become time wasters and sources of errors. The phenomenon of having two or more versions of a spreadsheet with inconsistent data is so common that it has given rise to its own term: dueling spreadsheets. This problem occurs because spreadsheets aren't bound to a single, unified source. Even if the original data is downloaded from the same place, such as an enterprise resource planning system, collecting it at different times can result in mismatched spreadsheets. Additions or deletions made to some versions but not in others can create variances.

EUC solutions can be risky with respect to data breaches. Many EUC solutions extract data from a production database into the EUC solution. The data then become much less secure, because the application can be stored on a user workstation, laptop, or external storage device.

2.3.4 Maintenance

During the development phase of an EUC solution, normally proper care is being taken that all the formulas and functions are intact and working as needed. Overtime as data grows and copy-paste takes place, EUC solutions will change more and more. At times the EUC solution might not work the way as it should. Most of the time this is the result of damaged formulas, broken links, and/ or overwritten cells.

A formal change management process and thoroughly verifying the integrity of EUC solutions are activities that many users do not want to perform. The effect is that errors slip in unnoticed. Studies have shown that errors persist, even when experienced professionals have examined them to spot errors in data, formulas, and broken links (Panko, 2008).

Regulators and external auditors have raised their concerns regarding EUC solutions during the last years for the same reasons that users love them. Their ease of use and manipulation makes them highly prone to errors and risk. Errors in EUC solutions can lead to inaccurate outputs and wrong results, which in turn can result in poor business and strategic decisions.

2.4 Big losses caused by using EUC solutions

Searching the Internet on losses caused by errors in EUC solutions gives a large number of search results. However, not all big EUC solution errors are made public. Also quantifying the loss due to errors in EUC solutions seems to be difficult.

Errors in use and formatting

In 2008, Barclays Capital used a spreadsheet to determine which assets belonging to Lehman Brothers it wished to buy after Lehmans' bankruptcy. In the rush to file before the bankruptcy court deadline, however, errors were made in spreadsheets use and formatting caused Barclays to list assets in the final purchase. As a result of this error, Barclays had to file a legal motion excluded 179 Lehman contracts worth several million dollars that were mistakenly included in the asset purchase agreement.

Errors in formulas

In 2005, Eastman Kodak was forced to restate financial results due to a spreadsheet that incorrectly calculated severance and pension related termination benefits.

Unauthorized changes

A trader in a major European bank was recently able to conduct a series of unauthorized trades – leading to $691 million in losses – by editing the spreadsheets used to monitor his unit's activities.

Error in manual data entry

The London 2012 organizing committee (LOCOG) confirmed that a decidedly unsynchronized error in its ticketing process had led to four synchronized swimming sessions being oversold by 10.000 tickets. LOCOG and its ticket agent Ticketmaster spent the Christmas period contacting ticket holders and offering them alternatives, starting with tickets for sports they had applied for but been unsuccessful.

LOCOG said the error occurred in the summer, between the first and second round of ticket sales, when a member of staff made a single keystroke mistake and manually entered '20.000' into a spreadsheet rather than the correct figure of 10.000 remaining tickets. The error was discovered when LOCOG reconciled the number of tickets sold against the final layouts and seating configurations for venues and began contacting ticket holders before Christmas.

Errors in formulas

Due to a calculating error by their financial advisors, West Baraboo officials learned that they will be paying about $4.000.000 more over the lifetime of their most recent 10-year borrowing plan than originally projected.

During its regular December meeting, the West Baraboo Village Board looked back over last month's decision to sell $1.1 million in general obligation bonds to cover a variety of village projects, said Village Clerk Mary Klingenmeyer. The review was required after the board received a letter from its financial advisory firm, Ehelers of Brookfield. Ehelers advisor James Mann said "operator error" resulted in a spreadsheet underestimating the total cost of the 10-year bond. "When we re-looked at the numbers we discovered a cell was not across the line being added correctly," he said. "So, it understated the impact."

2.5 Regulation in EUC context

2.5.1 GDPR

The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Implementing appropriate organizational and technological safeguards on all master production systems that contain personal and sensitive personal data is essential. But it is not enough. Personal data is often stored and analysed in EUC solutions. Storing the EUC solution in a local folder that is synchronized to a cloud storage service like Box, Dropbox, or OneDrive for Business is likely to compromise GDPR mandates.

Considering the massive volumes of data that exist in unstructured forms across the organization, a technological response to identify, catalogue, and classify all such data sources is an essential step, laying the foundation for taking appropriate action on any and every form of personal data thereby identified.

Human errors when sharing data in EUC solutions, is a high risk regarding the GDPR. Often, employees send spreadsheets containing customer names and personal information to management, other departments or external parties via e-mail. When a spreadsheet is accidentally sent to the wrong e-mail address, a data breach occurred and the GDPR regulation requires organizations to analyse the data breach and determine whether the data breach needs to be reported to the authorities.

2.5.2 Solvency II

Solvency II is the EU's initiative to reform regulation of insurance companies, by providing a consistent standard of capital requirements and risk management standards with the goal of increasing protection for policyholders. In January 2016, Solvency II was implemented by the 28 EU Member States plus three of the European Economic Area (EEA) countries, and the UK.

The Solvency II Directive identifies areas of need where an effective EUC solution management system is crucial including: risk management, data directory, data quality, change management, approval processes, security, version control and documentation. In each of these areas, the Solvency II regulation states specific requirements for compliance and companies need to ensure they have a sufficient system in place.The Prudential Regulation Authority (PRA) (formerly, the Financial Services Authority or FSA), published several findings and guidelines highlighting issues they encountered when reviewing current controls on spreadsheets and EUC tools. In addition to the directive itself, "Solvency II: internal model approval process data review findings" presents audit-based findings regarding the control of spreadsheets. This is highlighted by one finding in particular:

"Where EUC tools, such as spreadsheets, are material to the internal model data flow, we will be looking for appropriate controls for data quality such as reasonableness checks, input validations, peer reviews, logical access management, change and release management, disaster recovery, and documentation."

To be compliant with Solvency II requires an adequate risk management system to control the risks of using EUC solutions.

2.5.3 Sarbanes-Oxley

After financial reporting scandals at Enron and other major companies, the U.S. Congress passed the Sarbanes–Oxley Act (SOX) in 2002. Section 404 of the Act requires nearly every public company's chief corporate officers to assess whether the company's financial reporting system was effectively controlled during the reporting period. Furthermore, it specifies that the company must hire an independent external auditor to assess the officers' assessment. The focus of SOX and of Auditing Standard 2 is the creation of effective controls.

Controls cannot guarantee that the goals will be met, but they reduce the risk that these objectives will not be met. In this context, effectively controlled financial reporting processes give reasonable assurance that the company will meet the goal of producing accurate financial reports.

Auditing Standard No. 2 clarifies that controls must involve all forms of information technology (IT) used in financial reporting. One particular IT concern for corporations is the use of spreadsheets in financial reporting.
SOX brings the issue of controls on end-user developed spreadsheet models to the forefront as they make publicly traded companies accountable for verifying that effective controls for spreadsheets used in the financial reporting process are in place. In order to comply with SOX, companies need to document, evaluate, and test internal controls for spreadsheets that are critical for financial reporting.

2.6 Incentives to implement EUC solution risk management

The main objective of an enterprise EUC program is risk management. As with most risk management initiatives, the benefits (particularly those with hard dollar savings) can be difficult to quantify. However, many organizations that have deployed such programs have experienced bottom-line benefits in addition to risk mitigation, and they have developed business cases that demonstrate real return on investment (ROI). The experience with such programs leads us to conclude that the following benefits can be achieved:

- Reduced errors in preparation of financial statements and management reporting, resulting in faster closing processes and reduced staff time to research and remediate issues.
- Reduction in direct identified losses due to errors.
- Reduction in testing requirements and fees by auditors.
- Reduced regulatory and compliance penalties.
- Reduced training and on-boarding requirements for new employees.
- Elimination of redevelopment work needed to re-create EUC solutions when key employees leave, or when the EUC is lost.
- Opportunities to eliminate certain EUC solutions completely by identifying those that are organizationally entrenched but serve no direct business need, or that can be replaced by existing ERP functionality.
- Reduced effort to remediate errors in EUC solutions.

2.6.1 Mitigating controls

The implementation of controls is needed to be able to mitigate the risks of using EUC solutions. Basic spreadsheet programs lack the embedded logic and data controls necessary to prevent errors and misuse during operational use, so organizations need to apply manual or automated processes to help mitigate EUC solution risks during the entire life cycle (Coster et al., 2011).

General types of controls that can be considered include change controls, version controls, access controls, input controls, security and integrity of data, documentation, development lifecycle, back-ups, archiving, logical inspection, segregation of duties, and overall analytics (PriceWaterhouseCoopers, 2004).

Controls on entity level are not mentioned in this list. However, Lemon and Ferguson (2010) defined a more holistic framework based on a large case study. The framework includes governance, policies (including design standards), procedures, inventory management, and awareness. Hill and Barnes (2011) emphasize that large organizations should focus on two efforts to make sure that EUC solutions are properly controlled. The first effort is to establish controls over the development of EUC solutions. This includes a policy, communication, and training. The second effort is examining the EUC solutions itself. Examining EUC solutions exists of gaining knowledge of the EUC solutions that exist (inventory) and testing the EUC solutions for accurate processing.

2.7 Conclusion

The theoretical research provided us insights in what EUC solutions are, why organizations lean so heavily on them, and to what risks organizations are exposed when using EUC solutions for their primary businesses. The main goal of this chapter was to research which controls organizations should implement to mitigate the risks of using EUC solutions. To achieve this, we have elaborated on which risks organizations face when using EUC solutions. It is very unlikely that organizations will ever be able to completely exile EUC solutions from their businesses. Therefore, controls within a holistic risk management approach are needed to control the environment in which EUC solutions exist.

Based on our theoretical research we noted that suggested EUC solution risk management controls have a certain overlap with more formalized and mature application development and management processes. Therefore, creating a new control framework and reinventing the wheel to manage the risks of EUC solutions should not be needed. Instead, using existing IT development and management control frameworks like ITIL, CobIT, and ITGCs should cover a significant part of the risks that may materialize when using EUC solutions.

However, several nuances should be considered when creating a holistic EUC solution risk management approach:

- EUC solutions are not developed by mature IT departments with analists, architects, and other IT specialists.
- The business may be unaware of the risks of using EUC solutions.
- End users may resist against formalization of EUC solution development.
- Senior management may unconsiously stimulate the usage of EUC solutions by means of ad hoc reporting requests or providing insufficient budget for implementing mature applications.
- The ease of creation by end users makes it hard to manage the inventory of EUC solutions.

These nuances show us that attention for awareness, an adequate level of knowledge, preventive and entity level controls is very important besides more general controls like access, change, and continuity management.

To be able to create a holistic risk management approach we should also consider how organizations manage the risks of using EUC solutions in practice. By performing an analytical research, we can investigate what is needed to develop an approach like this but also wat the necessary steps are to make the approach effective in the longer term.

Merging the findings of the theoretical research together with the analytical research helps us to define how organizations may design and implement an approach to effectively manage the risks of using EUC solutions. In the next chapter we will elaborate on EUC risk management in practice, followed by an analysis and merging theory and practice.

3 Case study analysis and conclusions

The organization in scope of our case study (hereafter: GlobalCompany) is dealing with many different legacy IT systems. Most of these systems were developed in-house. The lack of flexible IT systems currently hinders GlobalCompany to be able to timely adapt its business in line with the rapidly changing markets and customer demands. At this time, GlobalCompany is therefore in a transformation process to become more digital and agile. One of the initiatives to leverage this transformation is the implementation of a new ERP system.

By performing a case study, research has been conducted on which controls organizations implement in practice to manage the risks of using EUC solutions. The controls identified during the case study have a certain overlap with existing IT general controls that were also identified during the theoretical research. However, some additional controls have been implemented besides specific EUC solution controls. Therefore, we distinguish two types of controls in this paragraph; entity level EUC solution controls and specific EUC solution controls.

3.1 Entity level EUC solution controls

GlobalCompany implemented several controls that can be described as entity level EUC solution controls. However, GlobalCompany does not have a control framework in which these controls are defined and monitored. Therefore, the implementation of this controls can be characterized as more ad hoc than mature by means of formalization and monitoring and improvement. The following entity level controls have been noted during the case study:

Policy

In line with the corporate policy, GlobalCompany defined a local policy regarding EUC solutions. The policy contains a description of the definition of EUC solutions. Also, roles and responsibilities within regarding EUC solutions are defined. Ensuring a complete list of all EUC solutions is part of the policy as well as periodic monitoring on the operational effectiveness of implemented controls.

Ownership

The Information Security Officer (ISO) is responsible for the management of risks regarding EUC solutions as the owner of the local EUC solution policy. The Chief Financial Officer (CFO) is accountable, since the ISO directly reports to this senior management function. As stated above, roles and responsibilities regarding EUC solutions are defined in the policy. Team leads of departments are responsible for implementing controls and maintaining the inventory of EUC solutions. Team leads are also responsible for reporting new EUC solutions to the Information Security team before using them. The Information Security team is responsible for supporting the business, performing reviews periodically, and assessing the adequacy of used controls.

Awareness

Several actions have been performed by GlobalCompany to create awareness regarding EUC solution risks. The activities had a focus on ensuring that current EUC solutions are included in the set of requirements for the new ERP system. Also, awareness has been created when departments were asked to follow-up on the risk mitigation approach by elaborating on the background and risks of using EUC solutions.

3.2 Specific EUC solution controls

Based on desk research and experience in the field of IT auditing, GlobalCompany created a set of controls which are mandatory to be implemented on each spreadsheet. As stated before, these controls have a certain overlap with existing IT general controls. The control categories below were defined. Within each category, controls were described in detail and shared with operational departments.

- Incorporated sheet in the EUC with general information
- Security and integrity of data
- Development and change management
- Availability management

3.3 What does a practical EUC risk management approach look like?

During the last years, several activities were performed by GlobalCompany to mitigate the risks of using EUC solutions. However, it never led to an effective and holistic approach. Since awareness on senior management level has been created as a result of several audit findings, GlobalCompany used a top-down approach to initiate a new way of working. Regardless of the suitability of this motive, it resulted in a starting point to develop and implement an EUC solution risk management approach. A certain level of awareness on senior management level was needed to allocate enough and capable resources that can effectuate a change. The ISO and an IT auditor were allocated and started with the development of the approach.

A phased approach was used by GlobalCompany to start managing the risks of using EUC solutions. By means of the case study, this research noted that the following activities were defined:

- Risk classification and prioritization
- Control definition
- Inventory management
- Control implementation
- Review and approval
- Monitoring and improvement
- Awareness

By starting with risk classification and prioritization, GlobalCompany was able to develop a ‘learning by doing’ way of working. Gained experience in practice was used immediately to optimize the approach before other departments were involved. The project started with a focus on departments that use EUC solutions for financial (reporting) purposes. However, the generic applicability of the approach made it possible to roll it out to other departments like Marketing and Commerce.

To reduce the number of EUC solutions within GlobalCompany, several awareness sessions have been organized. These awareness sessions had a major focus on the members of the ERP SYSTEM build and deployment project team. This team was responsible for defining requirements for the new ERP SYSTEM. The goal of the sessions was to ensure that EUC solutions used to overcome missing functionalities in the legacy software were translated to requirements for the new system.

3.4 Conclusions

Based on the case study at GlobalCompany and the analysis of the results, we have drawn the following conclusions:

Awareness on all organizational levels is a prerequisite

In the last years, employees of GlobalCompany performed several actions to start mitigating the risks of using EUC solutions. However, implementing a holistic approach and implementing controls did not take off for a longer period. The main reason for this was the lack of awareness, a low level of recognition of the importance, and the lack of available resources. However, when several audit findings were reported to the senior management, the awareness and recognition of importance increased. This resulted in a top-down approach and more priority was given to develop and implement an EUC risk management approach. Needed resources were made available to execute the approach. Awareness on operational level was created by the employees that were responsible for implementing the EUC risk management approach.

Ownership is key

GlobalCompany was able to give more priority to developing and implementing an EUC risk management approach by starting with ownership on senior management level. GlobalCompany accomplished this by making the Chief Financial Officer (CFO) the owner of the audit findings. The management team is encouraged to solve audit findings since open audit findings are directly linked to KPIs and targets. The CFO delegated the responsibility to implement the EUC risk management approach to the ISO. The CFO also prioritised the execution of the risk management approach within the Finance department. The development and implementation of the EUC risk management approach was added as a target in the personal development plan of the ISO. Also, the ISO was instructed to inform the CFO (escalate to senior management) in case of lack of cooperation from the Finance department. By means of a policy, ownership and responsibilities can be formalized.

Entity level as well as specific controls are needed

GlobalCompany defined and formalized a detailed set of EUC specific controls based on existing IT general controls but tailored to spreadsheets. These controls can be easily incorporated in a risk and control framework. Also, several entity level controls were implemented. However, besides an EUC policy describing roles and responsibilities, the entity level controls were not formalized and no part of a formal risk and control framework.

Risk classification needs to be specific

GlobalCompany users encountered difficulties in determining the risk of specific EUC solutions. Several risk classification approaches are defined by different studies, but GlobalCompany did not define its own risk classification approach.

Make it practical and provide support

One of the key success factors of the GlobalCompany EUC risk management approach was to make it as practical as possible. By creating a detailed manual including a best practice EUC solution, departments were able to follow a step-by-step approach. Also assigning specialists to the different categories of controls to provide support, facilitated the business to implement the mitigating measures.

New EUC solutions are created continuously

After performing the case study, we concluded that managing the risks of EUC solutions comes close to trying to empty the ocean with a thimble. Because of the organizational mindset, new EUC solutions are

created in a high frequency. Therefore, GlobalCompany created a certain level of awareness and provided the tools and knowledge to develop new EUC solutions in a safe and controlled manner.

Ensure periodic communication and reviews
To ensure that the risks of using EUC solutions are adequately mitigated, it is very important that the topic is kept at the top of mind of end users. GlobalCompany experienced a decrease in awareness and level of importance at business departments when the driving forces of the EUC risk management approach reduced their involvement.

4 Analysis of theory and practice

Chapter 2 and 3 are used to determine which recommendations can be given to implement an approach to adequately manage the risks of using EUC solutions. Taking these recommendations into consideration, brings us one step closer to answer the main research question of this research. The recommendations below are deducted from the theoretical as well as the analytical research.

Ensure a holistic approach
Based on our theoretical and analytical research, we concluded that a holistic approach is important to not only mitigate the risks of existing EUC solutions, but also to prevent the creation of new uncontrolled EUC solutions. With holistic we mean that the entire lifecycle of EUC solutions should be managed from design to maintenance (refer to figure 2.1). Holistic also refers to the need for entity level controls as well as EUC solution specific controls. Entity level controls are crucial to manage the creation of new EUC solutions. EUC solution specific controls have a certain overlap with IT general controls and are needed to mitigate the risks of existing EUC solutions.

Use a top-down approach
Managing the risks of EUC solutions is not only about implementing controls. Just as important is changing the organizational mindset. Support from senior management can be considered as a key success factor to effectuate this change. During our analytical research, we noted that a certain level of resistance can be experienced from end users when implementing an EUC solution risk management system. End users may not see the advantages of implementing controls. Also, implementing controls might hinder end users from benefitting of the advantages of EUC solutions.

Senior management has an important task in managing the risks of EUC solutions. They should ensure that enough EUC solution specialists are available to deal with organizational demands that motivates the creation of new EUC solutions. Also, sufficient IT budget should be available to minimize the need for EUC solutions by developing applications with a more mature and formalized development process. This also means that enough resources should be available to develop and implement changes in existing software. A top-down approach should result in ownership on strategic, tactical and operational level. Senior management, middle management and operational employees are all responsible for maintaining the risk management approach.

Create awareness on all levels
The previous recommendation endorses a top-down approach. However, this should be combined with creating a certain level of importance. Our analytical research showed us that the level of importance reduced significantly when the drivers of the implementation of the risk management approach diminished their involvement. Therefore, it is important that all stakeholders are aware of the risks, even when no one is watching. Periodic communication may help to maintain the needed level of awareness.

Provide adequate support to end users
Support is crucial to effectively implement EUC solution specific controls. Users are able to find their way in Excel but are usually less experienced in securing spreadsheets and implementing controls like change management, access management, and availability management. Therefore, the support of specialists is recommended in combination with a detailed manual and an example (best practice) of an EUC solution

with implemented controls. Support in determining the risk level of EUC solutions can also be recommended.

We also suggest that a design and development policy is created and communicated to ensure that end users are aware of the design principles and the needed controls. The policy should be approved by senior management and reviewed periodically.

Implement a monitoring and improvement process
As stated before, the level of importance can reduce easily when attention decreases. Besides, when policies, guidelines and manuals start deviating from reality, resistance against the approach can easily start to rise. Therefore, implementing a monitoring and continuous improvement process is important to avoid that the initiative to start mitigating the risks of using EUC solutions is a one-off exercise. A one-off exercise will not improve the risk mitigation on a long term.

Periodic independent reviews or audits may support the organization in keeping the importance of managing spreadsheet risks on top of mind.

5 Recommendations

After performing a theoretical and analytical research we have been able to merge theory and practice and define several recommendations that can be used to mitigate the risks of using EUC solutions.

At the start of this research we noted that many studies have already been performed on EUC in general and more specific on EUC solution risk management. However, a holistic and practical approach for developing, implementing, and maintaining an EUC risk management system was not yet available. By performing this research, we aim to provide insights in how organizations can implement an approach to effectively manage the risks of using EUC solutions and provide recommendations.

In paragraph 5.1 we concluded that implementing an EUC solution risk management approach is not a one-off exercise. Instead, continuous monitoring and improvement is needed to ensure that risks of using EUC solutions are mitigated effectively and ongoing. Continuous improvement and the 'plan, do, check, and act cycle' (also referred to as PDCA cycle, Deming cycle, or Shewhart cycle) are often mentioned in one sentence. The cycle is known worldwide and can be considered as an international best practice. Therefore, we decided to use this cycle to structure our answer on the main research question.

5.1 Plan (preparation and the development of a roadmap)

Implementing an approach to effectively manage the risks of using EUC solutions starts with a certain level of importance, awareness and support. Organizational risk appetite, legal obligations, major (financial) incidents, and/ or audit findings may have a significant influence on this importance. No matter what the motivation is to start developing a risk management approach, support on senior management level can be considered as a major success factor. Senior management should be aware that EUC solutions will probably never go away completely. Therefore, an approach to mitigate the risks of using them should be on their agenda.

EUC solutions are created by end users for numerous reasons. Awareness on senior level needs to be created regarding the motivation of end users to develop EUC solutions instead of using IT developed and supported applications. By understanding this motivation, senior management will be able to limit the creation of new EUC solutions. For example, by providing sufficient resources to incorporate business requirements in IT developed and support software. Another example is to not encourage the development of EUC solutions by not requesting complex and ad hoc reports from operational departments, but that seems wishful thinking.

When a certain level of awareness is created on senior management level, the ambition level regarding EUC solution risk management should be defined and resources should be designated to realize the ambition level of senior management.

As stated before, EUC solutions will probably never go away completely. Therefore, a risk management approach needs to be developed and implemented based on the defined ambition level.

The following activities should be considered when developing the EUC solution risk management approach:

1. Define roles and responsibilities and ensure that ownership is created.
2. Create a roadmap to meet the ambition of senior management. The roadmap should include:
    a. Formalization of risk appetite/ ambition level
    b. Policy and process definition
    c. Inventory methodology development
    d. Risk and control definition
    e. Creation of a risk and control framework
    f. Risk classification approach (in case of distinction between different levels of control)
    g. Implementation of controls
    h. Support
    i. Review and approval
    j. Monitoring and continuous improvement
    k. Communication and awareness plan
3. Formal approvement of the roadmap by senior management including the needed resources to execute the roadmap.

In table 4.1 we elaborate in more detail on how to implement the different activities defined in the roadmap. We also provide additional recommendations on activity level in this paragraph based on our theoretical and analytical research.

5.2 Do (execute the roadmap)

After establishing the needed level of awareness and support from senior management and the definition and approval of the roadmap, the plan needs to be transferred to actions. In the table 4.1, we described how the roadmap activities should be executed. Also, additional recommendations are provided when applicable.

5.3 Check (perform reviews and audits)

As already defined in table 4.1 performing reviews and audits are important to determine the effectiveness of the EUC solution risk management approach. During our analytical research, we noted that the level of awareness and ownership regarding EUC solution risk management can decrease significantly when driving forces of the approach reduce their involvement. Therefore, performing reviews and/ or audits periodically is very important.

During our analytical research we also noted that appointing audit findings on senior management level may contribute the effectiveness of the top-down approach.

5.4 Act (follow-up on findings and align theory with practice)

After formalizing ownership and periodic reviewing/ auditing the effectiveness of the EUC solution risk management approach, it is very important that audit findings are solved within acceptable time frames. Also, it is very important to collect feedback from operational departments to ensure that policies, procedures, and guidelines are aligned with practice.

Ref.	What	How	Additional recommendations
4.1.1	Determine and document risk appetite/ ambition level	Discuss the risk appetite regarding the risks of using EUC solutions with senior management. Ensure that they understand the risks of using EUC solutions and the possible organizational impact in case of errors or (financial) incidents. Cooperate with other risk specialists/ departments (refer to ref. 6.1.4).	Consider organizing a risk assessment workshop with senior management.
4.1.2	Policy and process definition	Create an EUC solution policy which includes at least: - Owner - Responsibilities - Definition of EUC solutions - Related documents and guidelines - Monitoring and reviews Ensure that processes are documented in detail to ensure consistent approaches. Consider at least: - Inventory management (ref. 6.1.3) - Risk classification approach (ref. 6.1.7) - EUC solution change management and approval process	Ensure that policies and processes are reviewed periodically and formally approved.
4.1.3	Inventory methodology development	A complete list of EUC solution is necessary to effectively manage the risks of using EUC solutions. Define a methodology that suits the organization and consider the usage of available tooling to automate the inventory processes. Ensure that responsibilities regarding the completeness and correctness of the inventory are defined clearly (also refer to ref. 6.1.2).	Consider asking employees of departments to document each EUC solution that they use during a work day. After several weeks a complete overview should be available. Also consider creating a group EUC solution champions throughout the organization acting as ambassadors of the driving forces behind the EUC solution risk management approach.
4.1.4	Risk definition	Define risks in cooperation with risk specialists. Consider at least the following risk categories: - Financial risk - Operational risk - Information security risk - Privacy risk - Compliance risk	No additional recommendations applicable.
4.1.5	Control definition	Define entity level and specific EUC solution controls. Consider at least the following categories: Entity level controls - Governance - Policies (including design standards) - Procedures - Inventory management - Awareness Specific EUC solution controls - Documentation - Access management - Change management - Availability management	EUC solution controls have a certain overlap with controls in existing control frameworks (CobIT, ITIL, ISO 27001, etc.). Prevent wasting scarce resources on reinventing the wheel. Refer to table 3.2 for a list of controls implemented on EUC solutions by GlobalCompany.
4.1.6	Creation of a risk and control framework	Incorporate EUC solution risks (ref. 6.1.4) and controls (ref. 6.1.5) in existing business control framework to ensure ownership and monitoring.	Cooperate with other risk specialists/ departments (refer to ref. 6.1.4).
4.1.7	Risk classification approach (in case of distinction between level of control implementation)	Define a risk classification approach to determine the risk level of EUC solutions. The risk level can be used to choose the level of controls to be implemented. Consider the following classification possibilities: Likelihood - Complexity of the spreadsheet and calculations - Purpose and use of the spreadsheet - Number of spreadsheet users - Types of potential input, logic, and interface errors - Size of the spreadsheet Impact - Financial misstatement - Decisions - Invoicing	Be aware that risk assessment activities require a certain level of experience in the field of risk management. Providing support to end users would therefore be recommended. Risk assessments also require a certain level of professional judgement. Try to not spend too much scarce resources on determining the likelihood and impact in too much detail.

Ref.	What	How	Additional recommendations
4.1.8	Implementation of controls	Determine when the controls need to be implemented on existing EUC solutions. Also consider who is responsible for implementing the controls.	Consider a phased approach to be able to make adjustments and improvements. Another advantage of a phased approach is less organizational impact.
4.1.9	Support	Provide sufficient support to operational departments to reduce the risk of resistance or low-quality control implementation. Consider at least the creation of a detailed manual, a best practice EUC, and an EUC development guideline (may overlap with the manual). Also consider making EUC solution specialists available for end users to support the implementation of controls.	Many best practices are available online. Prevent wasting scarce resources on reinventing the wheel.
4.1.10	Review and approval	Ensure that a review and approval process is performed on each EUC solution. This process differs from the change management process (ref. 6.1.5) but helps to ensure that the change management process is operating effectively. The review and approval process need to be created to monitor the effectiveness of implemented controls and to ensure that only approved EUC solution are used.	Determine who is responsible for reviewing and approving each EUC solution. Organizations may decide not to have senior management review and approve all EUC solutions that are in use. The considerations and decisions should be documented in ref. 6.1.2.
4.1.11	Monitoring and continuous improvement	Ensure monitoring and continuous improvement by the second as well as the third line. Cooperate with the internal audit department to ensure that periodic audits are performed on the effectiveness of the EUC solution risk management approach. Since policies, procedures, the risk and control framework are defined, the internal audit department may use this as a norm to perform audits. Also, external audits may be used to determine the effectiveness of the EUC solution risk management approach.	Several studies are performed on auditing EUC solutions. Prevent wasting scarce resources on reinventing the wheel.
4.1.12	Communication and awareness plan	Develop a communication plan to ensure periodic and effective communication. Consider at least: - Target group - Communication methods - Planning/ schedule	No additional recommendations applicable.

Table 4.1: Activities to implement an EUC risk management approach (roadmap)

6 References

Alavi, M., & Weiss, I.R. (1985-1986). *Managing the Risks Associated with End-User Computing*. Journal of Management Information, 2(3), 5-20.

Baškarada, S. (2011). *How Spreadsheet Applications Affect Information Quality*. The Journal of Computer Information Systems, 51, 77-84.

Bellino, C. A., Ochab, D., & Rowland, J. S. (2010). *Global Technology Audit Guide (GTAG): 14 Auditing User-developed Applications*. The Institute of Internal Auditors.

Brancheau, J., & Brown, C. (1993). *The Management of End-User Computing: Status and Directions.* ACM Computing Surveys, 25(4), 437-482.

Coster, N., Leon, L., Kalbers, L., & Abraham, D. (2011). *Controls over Spreadsheets for Financial Reporting in Practice*. Proceedings of EuSpRIG 2011 Conference.

Deloitte. (2009). *Spreadsheet Management: Not what you figured*. Deloitte.

Hall, M. (1996). *A Risk and Control Oriented Study of the Practices of Spreadsheet Application Developers*. Proceedings of the 29th Hawaii International Conference on System Sciences, 364-370.

Hermans, F., Pinzger, M., & Deursen, A. van. (2012). *Detecting Code Smells in Spreadsheet Formulas.* ICSM 2012: 409-418.

Hill, M., & Barnes, W. (2011). *End-User Computing Applications*. The CPA Journal, 81(7), 67 71.

Jenne, S. E. (1996). *Audits of End-User Computing*. Internal Auditor, 53(6), 30-34.

Leitheiser, R. R., & Wetherbe, J. C. (1986). *Support Levels: An Organized Approach to End User Computing*. MIS Quarterly, 10, 337-349.

Lemon, T., & Ferguson, E. (2010). *A Practical Approach to Managing Spreadsheet Risk in a Global Business*. Protiviti
Limited.

O'Regan, G. (2012). *A Brief History of Computing (2nd edition)*. Springer-Verlag London Limited.

Panko, R. R. (2006). *Spreadsheets and Sarbanes-Oxley: Regulations, Risks and Control Frameworks*. Communications of the AIS, 17, 1-50.

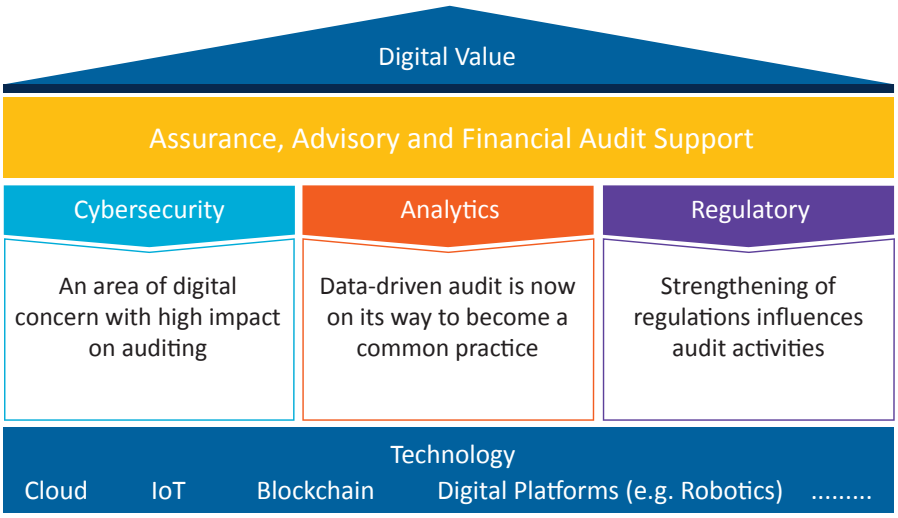
Panko, R. R. (2008). *What we know about spreadsheet errors.* Journal of End User Computing's Special issue on Scaling Up End User Development, pp. 15-21.

PriceWaterhouseCoopers. (2004). *The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act.* PriceWaterhouseCoopers.

Romney, M., & Steinbart, P. (2006). *Accounting Information Systems*, 10th ed. Pearson Education Limited.

Ruparelia, N. B. (2010). *Software Development Lifecycle Models*. SIGSOFT Software Engineering Notes, 35, 8-13.

HOUSE OF IT AUDITING



International Federation for Information Processing

TC-11

Security and Privacy Protection in Information Processing Systems

9 789082 851717

EDITION 2019