Determining the Benefits of Continuous Monitoring

A Tool for Prioritizing Internal Controls during a Continuous Monitoring Implementation

---

Master Thesis

Rãzvan Turtoi
Master of Business Informatics
Department of Information and Computing Sciences
Utrecht University, the Netherlands

master of
business informatics
utrecht university

Determining the Benefits of Continuous Monitoring

A Tool for Prioritizing Internal Controls during a Continuous Monitoring Implementation

Author	Rãzvan Turtoi
StudentId	3563618
E-mail	turtoi.razvan@gmail.com
Date	9 October, 2012
Utrecht University Supervisors	dr. Marco R. Spruit
	dr. ir. Remko W. Helms
BWise Supervisors	dr. Luc Brandts
	drs. ing. Anton Lissone

ACKNOWLEDGEMENTS

This report represents the research I carried out for the period of seven months as a graduation project of the Business Informatics master program at Utrecht University. This research represented a collaboration between Utrecht University and BWise, and I would like to acknowledge a number of people.

I would like to thank my Utrecht University supervisors, Marco Spruit and Remko Helms, for offering me guidance and for attention to detail. They reviewed my work and provided me with constructive comments and insights.

Additionally, I would like to thank my BWise supervisors, Anton Lissone and Luc Brandts, for offering me this opportunity and investing their time and knowledge throughout this research every time I needed it. I would also like to thank the colleagues in the R&D department at BWise for creating a pleasant working environment.

Furthermore, I would like to thank all the experts that I interviewed for their valuable feedback and all the respondents of the online questionnaire. Thank you to the two organizations that agreed to participate in this research by agreeing to help me and providing their data.

Lastly, I would like to thank my parents, Constantina Bratu and Aurel Turtoi, for their love and support. I also want to thank my friends, Vlad Buda, Ana Stroe, Maria Suciu, Thodoris Polychniatis, Andrei Idu, Elizabeth Zeller and Lisa Ströter, that offered me their support and feedback on my work. Last but not least, I want to thank my master colleagues for their feedback during the colloquium sessions.

ABSTRACT

The research area of Continuous Monitoring (CM) is rather manifold. The concept of CM has emerged as a link between corporate governance, financial reporting, audit, internal control and IT. In order to meet compliance and operational objectives, organizations establish internal systems that categorize the most important risks, with all the necessary mitigating measures, entitled controls. Together, the controls should provide reasonable assurance that the business is in control. Publicly traded companies develop internal control systems with the main purpose of providing accurate financial statements that portray the reality as it is. In order to do that controls must be tested on a regular basis. Due to the high amount of work required, it has become an auditor's task instead of the controller's duty. For that reason, extensive academic work exists on the topic of audit, more precisely on Continuous Auditing (CA). CA refers to the use of system-based techniques that replace the manual audit ones. Although CM has emerged with an identical meaning as CA, a clear delimitation started to be observed over the past years between the two. Although no generally accepted terminology exists on CM, they all refer *"a process to ensure that policies and processes are operating efficiently and to assess adequacy and effectiveness of controls"* (CICA/AICPA, 1999).

The recent technological advancements make it possible for the controllers to monitor their controls on a regular basis, and provide evidence to the audit whether controls are functioning as intended, and what steps are performed in case exceptions are encountered. One example of a control is the three-way match. The amount of goods ordered, the amount of goods received, and the amount of goods invoiced, together with their value must match. Although the three-way match setting exists in most ERP systems, due to their complexity, it is assumed that this setting is enabled. CM provides complete assurance whether such a setting is enabled or not, and, most importantly, examines the entire population of transactions to check whether there are any three-way mismatches.

Due to the significant amount of controls that organizations set, it is unclear on which controls to focus first in a CM implementation project. Consequently, this research proposes an internal control prioritization tool that would identify and relate the relevant dimensions in order to prioritize a set of controls. In order to evaluate the results of the framework, two case studies are used. Challenges of adopting CM technology are identified by the means of a questionnaire. A clear picture of what CM represents is presented by performing extensive literature study various discussions within BWise and expert interviews.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

Chapter 1 Introduction

This graduation thesis describes the research carried out on the topic of Continuous Monitoring. The concept of Continuous Monitoring is defined by CICA/AICPA (1999) as *"a process to ensure that policies and processes are operating efficiently and to assess adequacy and effectiveness of controls".* Teeter and Brennan (2008) argue that automated continuous monitoring tools provide the means for *continuous control**s** monitoring* which is defined as the *"process of evaluating the effectiveness of internal controls in detecting errors and anomalies on an ongoing basis"*. Section 3.6 provides the reader with an in-depth understanding of this branch of data analysis technology.

The current research aims at identifying the parties that benefit the most from data analysis software tool implementation and the benefits identified by those parties. Moreover, the project also pursues to develop a tool that, applied on a list of internal controls, prioritizes a list of internal controls and provides a starting list of controls that is in scope for Continuous Monitoring implementation.

In this chapter, the research triggers are described and gaps in the current scientific body of knowledge are outlined. Section 1.1 contains the motivation that triggered this research topic, together with its objective and its problem statement. Section 1.2 presents the main research question and the adjacent five sub-questions. Section 1.3 contains the contribution of this research.

1.1. Motivation

The market disruptions in the late 1990s, economic crisis and financial turmoil in the early 2000s have led to an increasing amount of compliance standards, international and local laws and regulations that executives and corporations have to abide to. These compliance efforts lead to considerable material costs (Swartz, 2003; Carney, 2006) for companies, and do not assure the identification of all risks that can prevent companies from attaining their objectives. Considerable efforts are invested (i.e. people, time and money) by the business owners to understand and detect the risks that can appear. In order to monitor and/or mitigate those risks firms set up the necessary internal controls. The internal and external audit teams, on the other hand, assess the effectiveness and accuracy of the information in the financial statements and the evaluation of a system's internal controls. Even with all these initiatives in place, organizations still receive legal fines from regulators for not being able to close their compliance gaps and errors on a timely manner and, therefore, perform the necessary measures to mitigate them. In other words, their internal control system is ineffective. Consequently, the attention has turned to monitoring the effectiveness of those internal controls that are set in order to detect and limit the risks that might damage corporations when exceptions occur.

Nowadays, the technological advancements make it possible to start monitoring controls with the use of data analysis software tools, entitled Continuous Monitoring (CM). Organizations are convinced that this technology brings many benefits, but due to the unknown challenges of investing in a Continuous Monitoring implementation, large batch of controls that need to be implemented in a CM project, the difficulty of accessing Enterprise Resource Planning (ERP) systems (Alles, Brennan, Kogan & Vasarhelyi, 2006) and limited budget, Continuous Monitoring technology is sometimes believed to be unable to outrun the costs of implementation.

The research project was initiated at the Dutch software company, BWise[1], which operates under the NASDAQ OMX umbrella and is currently selling and developing a Continuous Monitoring solution. BWise is a leader in Enterprise, Governance, Risk Management and Compliance software (McClean, Balaouras & Hayes, 2011), supporting organizations worldwide in their various efforts of tracking, measuring and managing key organizational risks in one centralized system.

The objective of the current graduation assignment is to provide organizations with a tool that selects and prioritizes internal controls in order to maximize the return on investment of a Continuous Monitoring implementation project. At the same time challenges and preconditions when adopting this type of data analysis technology will be identified.

The large amount of specifications, policies, standards, laws, and best-practice frameworks, i.e. Sarbanes-Oxley (SOX) U.S. Act (SEC, 2002), ISO 27002 (ISO/IEC 27002, 2005), MIFID (European Commission, 2004), PCI (Payment Card Industry, 2010), have led to the creation of different focus areas within organizations forcing them to develop risk assessment strategies and hence a multitude of controls that reduce or eliminate the identified threats. In order to cut down on compliance costs and maintain competitiveness in the market, firms examine investments in tools that perform monitoring of their controls in an automated manner and on an ongoing basis. This leads us to the formal problem statement of this research endeavor is:

There is an increased amount of non-automated internal controls that require significant manual efforts and enterprise systems whose settings are not easily accessible (Alles et al., 2006).

A possible solution would be the use of Continuous Monitoring technology. As such, the formal objective of this research is:

To provide insight in what Continuous Monitoring technology represents, its perceived benefits and provide organizations with a tool that defines and relates the relevant dimensions in internal control prioritization.

[1] http://www.bwise.com/

1.2. Research Questions

Based on the problem statement introduced in Section 1.1, the main research question that will give an answer to the problem is formulated. The research question represents a consequence of the scarce scientific literature and empirical needs of continuous data analysis technologies.

The main research question is as follows:

RSQ: How can organizations be assisted in prioritizing their internal controls for Continuous Monitoring?

The main research question mentioned above is divided into several sub-questions to provide the reader with a clearer explanation of what the scope is and what the deliverables are. The sub-questions defined below investigate the various views of the problem statement.

RSQ1: What does Continuous Monitoring represent and what are the stakeholders that benefit the most from a Continuous Monitoring implementation?

This sub-question is answered by reviewing related literature in the field and one expert interview. A clear definition of what Continuous Monitoring is and the parties that benefit from it are identified. The review of scientific and managerial literature offers the researcher the necessary and sufficient theoretical background.

RSQ2: What are the most valuable gains from implementing a Continuous Monitoring software solution as distinguished by the identified stakeholders?

The answer to RSQ2 is provided by examining the existing literature and performing three semi-structured interviews. Based on the findings, an online questionnaire is assembled and sent to the parties identified in RSQ1 to be evaluated.

RSQ3: What are the challenges that organizations need to overcome when considering an implementation of Continuous Monitoring software tools?

Based on literature study and online questionnaire results, challenges that organizations need to overcome when considering a continuous data analysis software technology are identified and explained.

RSQ4: What are the relevant dimensions in internal control prioritization and how can they be related to each other?

An Internal Control Prioritization Tool is assembled with the information gathered from the literature study and expert interviews. The IT artifact is refined and improved by the means of expert interviews. In order to ensure the validity of the tool, the tool is applied on the Internal Control Matrixes of two publicly traded organizations.

RSQ5: How can the Internal Control Prioritization Tool be applied in practice?

In order to answer the last question, expert interviews are conducted in order to assess the validity of the tool and to provide feedback for possible improvements. Additionally, two case studies are performed and the results are discussed with the organizations for a final evaluation of the findings.

1.3. Contribution

1.3.1. Scientific Contribution

From an academic perspective, this project contributes to the overall knowledge on data analysis technology. Although extensive research has been conducted in the fields of corporate governance, financial reporting and continuous auditing, the focus was only on the benefits for the internal and external auditors. The evolution of new technologies has taken the traditional approach of audit from manual work to a more IT-centric approach, that of Continuous Audit (CA) (Searcy, Woodroof & Behn, 2003b). Although a definition for Continuous Monitoring emerged as early as 1999 (CICA/AICPA, 1999), CM is mentioned to have an identical meaning as CA (Kuhn & Sutton, 2010). An abundance of scientific work exists on the area of CM, but only from an auditor's point of view (Warren & Parker, 2003; Alles et al., 2006; Alles, Kogan, Vasarhelyi & Wu, 2008a; Alles, Kogan & Vasarhelyi, 2008b; Alles, Kogan & Vasarhelyi 2009; Henrickson, 2009).

Although differences between the two concepts started to be observed (ISACA, 2002; Warren & Parker, 2003; Daigle, Daigle & Lampe, 2008; Henrickson, 2009), to the best of our knowledge, no work has been observed in the academic body of knowledge regarding the benefits and challenges of CM, from a business/control owner's perspective. Another scientific relevance that sustains the contribution of this research to the academic body of knowledge is represented by defining and relating the relevant dimensions in internal control prioritization. These contributions will pave the way for future research in the field of Continuous Monitoring.

1.3.2. Social Contribution

The social trigger plays an important role in the initiation of this thesis project as well. With the introduction of stricter regulations, organizations worldwide have invested substantially in internal control systems in order to reach compliance, provide complete assurance of financial statements and identify possible business improvements opportunities. As the costs were considerable, frameworks were developed and implemented to be in control of one's organization and adhere to national and international laws. At the moment, Continuous Monitoring technology facilitates the monitoring of organizations' internal controls. This research provides a clear understanding into the field of internal controls, i.e. a picture of what CM represents, what are the main benefits, and how to determine which controls should be used as a starting point during a CM implementation. Hence, the research was triggered by business needs of a software company that offers CM capabilities, but also by organizations that are either at the moment or considering implementing in the future a CM software tool.

Chapter 2 Research Approach

The research question and sub-questions described in Chapter 1 are answered based on a research approach. The research approach is detailed in this chapter. Design science research (Hevner, March, Park & Ram, 2004) is the main research method used in the research project. The several activities that are performed to gather information provide sufficient knowledge to assemble the final deliverable and assess its validity. The results of this research yield both scientific and social contributions. On one hand, it covers the existing gaps in the scientific literature and, on the other hand, it helps corporations detect opportunities for improvements in their business processes and diminish financial losses.

The main research method is detailed in Section 2.1. Section 2.2 contains the activities that are performed to reach an answer to the research questions, while a high-level overview of the research instruments that were pursued in this thesis is presented in Section 2.3.

2.1. Design Science Research

The research approach is based on the research in design science in information systems. This approach was assembled by Hevner et al. (2004). According to Hevner et al. (2004), design science intends to contribute to the scientific body of knowledge by constructing new and valuable IT artifacts. Based on the stated problem and objective of this current research, the main deliverable, the challenges that arise when adopting a Continuous Monitoring software solution and the prioritization tool fit perfectly into the design science research requirement. The Information Systems Research Framework on which the current thesis is based was adopted from Hevner et al. (2004) and is depicted in Figure 1. In conjunction, March and Smith (1995) argue that design science not only facilitates the creation of an artifact but also helps evaluate it by introducing cycles of artifact development.

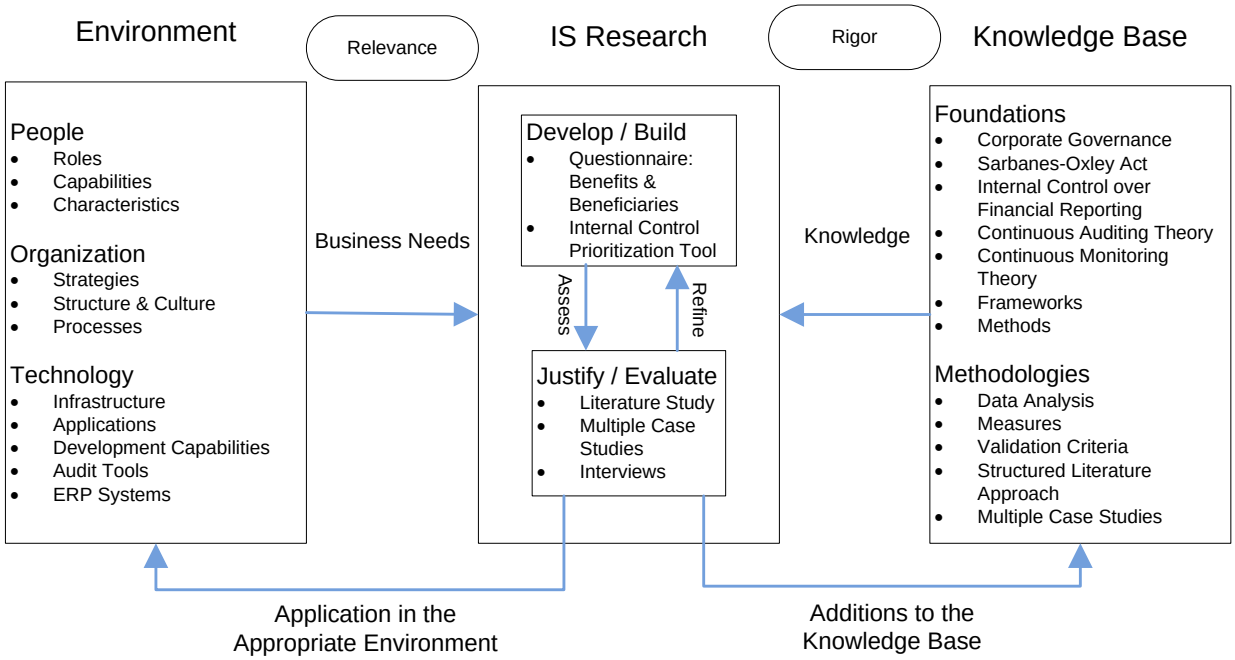

Figure 1: Information Systems Research Framework adopted from Hevner et al. (2004)

2.2. Research Planning

Takeda, Veerkamp, Tomiyama, and Yoshikawa (1990), and Vaishnavi and Kuechler (2007) provide a design cycle for this type of research, which is depicted in Table 1 and contains five design steps to be fulfilled as follows:

Table 1: Design cycle derived from Takeda et al. (1990) and Vaishnavi & Kuechler (2007)

Research Steps	Description
Problem Awareness	Identification of the problem and the reason for which a solution is needed.
Suggestion	Based on various findings, i.e. existing knowledge and theory and empirical research, suggestions from the problem identified in Step 1 are drawn.
Development	Based on the suggestions from the previous step, a solutions/artifact is proposed.
Evaluation	Partially or fully successful solutions are evaluated to observe whether they solve the stated issue. If that is not the case or the solution lacks consistency, the whole process flows back to Step 2.

Conclusion	An outline of the results is being presented and the design cycle is ended.

The current thesis is composed of five main stages. This section details each stage in a sub-section. In order to give a better view of the project's phases, the method initiated by Weerd and Brinkkemper (2008), known as method engineering, will be used. This outputs a process-deliverable diagram (PDD) and is presented in Figure 2. A PDD describes the processes of the methodology in terms of activities that need to be carried out and the deliverables that are the output of these activities. The activities are depicted on the left-hand side of Figure 2 and further detailed in Table 2, whereas the deliverables are depicted on the right-hand side of Figure 2 and explained in Table 3.

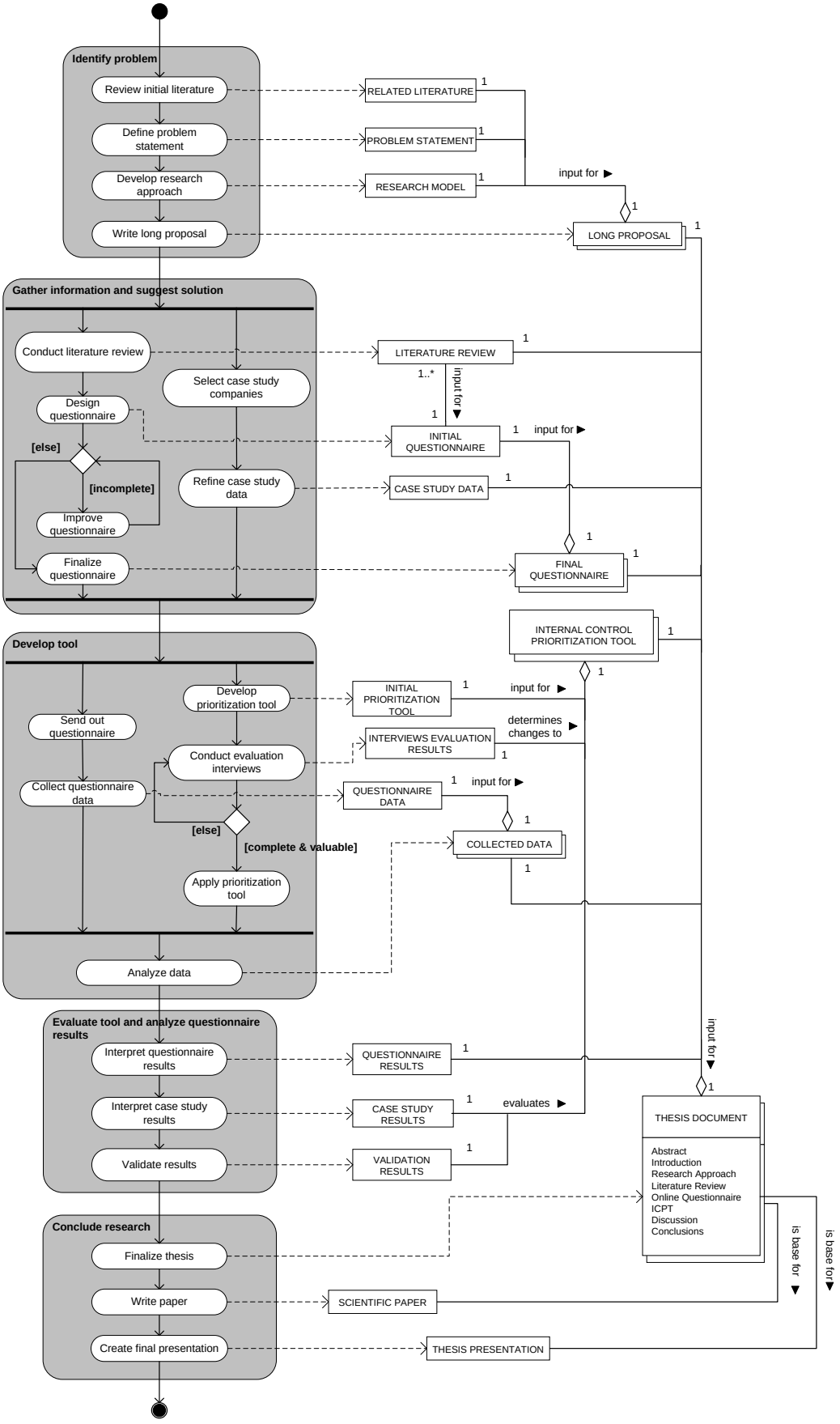

Figure 2: The thesis process-deliverable diagram

Table 2: Process-Deliverable Diagram Activities

Activity	Sub-activity	Description
Identify problem	Review initial literature	The RELATED LITERATURE is determined by performing an initial literature study and preliminary discussions with experts from the company that triggered this research.
	Define problem statement	Based on the initial literature review, the PROBLEM STATEMENT is identified.
	Develop research approach	The RESEARCH MODEL is established based on literature study on research methods in the IS field.
	Write long proposal	All the above sub-activities are merged into one document, the LONG PROPOSAL, and submitted for approval.
Gather information and suggest solution	Conduct literature review	After the LONG PROPOSAL was approved, literature study was carried out to obtain a solid understanding of the CM concept. The LITERATURE REVIEW was input for INITIAL QUESTIONNAIRE.
	Design questionnaire	Based on the findings from the literature study, an INITIAL QUESTIONNAIRE was assembled.
	Improve questionnaire	In order to improve the questionnaire, interviews were conducted with experts in the field. The process was stopped when the questionnaire was complete.
	Finalize questionnaire	All the feedback was thoroughly analyzed and a final version of the questionnaire was assembled, resulting into the FINAL QUESTIONNAIRE concept.
	Select case study companies	A list of potential participants was formed. The participants had to be listed on a stock exchange and have subsidiaries in multiple regions. E-mail requests were sent to the potentially interested organizations.
	Refine case study data	A number of organizations showed interest into the research, and it was determined that Internal Control Matrix containing processes, risks and controls used in their day-to-day operations were needed.
Develop tool	Send out questionnaire	Information containing the type of respondents needed for the questionnaire was formed and

		formal e-mails containing the online link of the questionnaire were distributed.
	Collect questionnaire data	The results of the respondents were collected into QUESTIONNAIRE DATA.
	Develop prioritization tool	Based on the analysis of the documentation of the two organizations involved in the case studies, an INITIAL PRIORITIZATION TOOL was constructed.
	Conduct evaluation interviews	Evaluation interviews with field experts were planned to refine and improve the tool. This sub-activity was carried out until the tool was valuable and complete.
	Apply prioritization tool	In this sub-activity, the prioritization tool was applied in two case studies data to ensure its applicability.
	Analyze data	The results of the application of the tool are gathered and all the available data is analyzed.
Evaluate tool and analyze questionnaire results	Interpret questionnaire results	The results of the questionnaire are presented in a clear and reliable manner.
	Interpret case study results	The results of the case study analysis are described.
	Validate results	The results of the case studies were presented to the participating organizations and their feedback was requested and analyzed.
Conclude research	Finalize thesis	All the data acquired from the above sub-activities are assembled into a single document. Additionally, discussion and conclusions are formulated.
	Write paper	Toward the end of the research, a scientific paper will be delivered and will be submitted to a journal/conference.
	Create final presentation	At the end of the research, the thesis will be presented and defended, resulting into a THESIS PRESENTATION.

Table 3: Process-Deliverable Diagram Deliverables

Deliverable	Description
RELATED LITERATURE	Literature study that provides background knowledge on the research topic.
PROBLEM STATEMENT	A description of the gaps identified in the scientific world and problems faced by organizations.
RESEARCH MODEL	A detailed description of all the steps carried out by the

	researcher.
LONG PROPOSAL	Contains the basic literature review, the problem statement, the objective, the research questions and the research approach.
LITERATURE REVIEW	Extensive literature study was conducted to gain a solid understanding at the topic at hand.
INITIAL QUESTIONNAIRE	A draft of the questionnaire was assembled based on literature review and expert interviews.
CASE STUDY DATA	It represents the data that was required from the participants of the scientific study.
FINAL QUESTIONNAIRE	It contains the statements and the target group for the online questionnaire.
INITIAL PRIORITIZATION TOOL	A draft version of the prioritization tool was compiled after a careful analysis of the CASE STUDY DATA.
INTERVIEW EVALUATION RESULTS	In order to improve the artifact, expert interviews were conducted.
INTERNAL CONTROL PRIORITIZATION TOOL	It represents a complete and final form of the artifact.
QUESTIONNAIRE DATA	Data from the respondents was extracted from the online environment.
ACQUIRED DATA	Questionnaire and case studies data were assembled and analyzed.
QUESTIONNAIRE RESULTS	The complete and detailed results of the questionnaire.
CASE STUDY RESULTS	The complete and detailed results of the case studies that evaluates the tool.
VALIDATION RESULTS	The complete feedback received from the organizations that evaluated the tool.
THESIS DOCUMENT	The final version of the thesis.
SCIENTIFIC PAPER	Paper written for submission to a journal or conference.
THESIS PRESENTATION	The presentation of the thesis.

2.3. Research Instruments

The development of a research strategy is the core of a valuable research endeavor. In this section the research instruments designed to accomplish the objectives during various phases of the project are described.

Table 4 contains the research questions and the corresponding research instruments that are employed to answer them.

Table 4: Research questions and instruments

Research question	Research instruments
RSQ1: What does Continuous Monitoring represent and what are the stakeholders that benefit the most from a Continuous Monitoring implementation?	Literature Review
	Expert Interviews
RSQ2: What are the most valuable gains from implementing a Continuous Monitoring software solution as distinguished by the identified stakeholders?	Literature Review
	Expert Interviews
	Online Questionnaire
RSQ3: What are the challenges that organizations need to overcome when considering an implementation of Continuous Monitoring software tools?	Literature Review
	Expert Interviews
	Online Questionnaire
RSQ4: What are the relevant dimensions in internal control prioritization and how can they be related to each other?	Case Study Documentation
	Expert Interviews
RSQ5: How can the Internal Control Prioritization Tool be applied in practice?	Case Studies
	Expert Interviews

Chapter 3 Literature Review

This chapter presents the literature study of this research. The research area of Continuous Monitoring is rather manifold as not one unique necessity led to its emergence. The concept of Continuous Monitoring has emerged as a link between corporate governance, financial reporting, audit, internal control and IT. The literature review on corporate governance, financial reporting and audit is meant to educate the reader on the origins of CM. Thorough literature study was performed with the scope of gaining solid background in the fields of internal controls and on the topic of CM. The literature research was undertaken in a semi-structured fashion for flexibility reasons, as it allows the researcher to dive into a larger set of data. In the subject of this project, flexibility was required taking into consideration the four fields that this topic aggregates Corporate Governance, Financial Reporting, Audit and Internal Control. Both academic literature and managerial literature contain sufficient publications that provide a clear and concrete landscape of the topic at hand.

Webster and Watson (2002) describe a literature study approach and guidelines on how to review preexistent and relevant literature. This approach best suited this research because of the three-step approach proposed by the authors. The first activity deals with identifying the main contributions in leading journals, publications and conferences. The second step performed was to analyze the citations referenced in the major contributions and go to the primary sources. In this way, previous articles and more detailed knowledge is acquired. Finally, recent literature is discovered by using academic content search engines that output papers that reference the already identified articles.

The literature is assembled by using Google Scholar[2] search engines. Secondary sources[3,4] were used to describe current governmental obligations. Prior experience of the researcher with the use of the Systematic Literature Study (Okoli & Schabram, 2010) helped to optimize the search efforts by explaining in an explicit manner to the reader of this research the search queries that were used to determine the relevant papers, by eliminating the articles of insufficient quality and by stating the reasons for doing so. The SLS represents "*a systematic, explicit and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars, and practitioners*". The search queries used a mixture of various terms as depicted in Table 5.

.

[2] http://scholar.google.com/
[3] http://www.sec.gov/
[4] http://www.coso.org/

Table 5: List of words used in search queries

Keyword	Nr of initial articles
"Initial Public Offering Analysis"	2
"Information Technology Sarbanes-Oxley"	4
"Continuous Auditing"	7
"Continuous Monitoring"	2
"Continuous Controls Monitoring"	4
"ERP System Sarbanes-Oxley"	3
"Corporate Governance Overview"	6
"Corporate Financial Reporting"	1
"Cost Sarbanes-Oxley"	2
"Internal Controls over Financial Reporting"	3
"Internal Control Framework"	2

Searches of major scientific works led to a number of 36 paper publications. Tracing the primary sources was employed by accessing the references of these publications. Based on this list, a follow-up of citations was performed by studying the papers which cite the papers in the initial list. As a result, the list size expanded. At this point, the abstract of each work was thoroughly read and the main content was quickly scanned before a consistent list resulted in 80 papers that were analyzed further. Analytical reports from Gartner[5] were studied to get a better grasp of the corporate environment.

3.1 Corporate Governance and Information Technology

Corporate governance represents a critical factor in determining a company's business success and its accountability. Zingales (1998) defines corporate governance, from a wide perspective, as "*the complex set of constraints that shape the ex-post bargaining over the quasi-rents generated by a firm*". Shleifer and Vishny (1997) describe corporate governance as the modalities by which investors assure themselves that their investments are getting a return in the future. According to Gillan and Starks (1998), corporate governance is viewed, in simpler terms, as "*the system of laws, rules and factors that control operations at a company*".

[5] http://www.gartner.com/

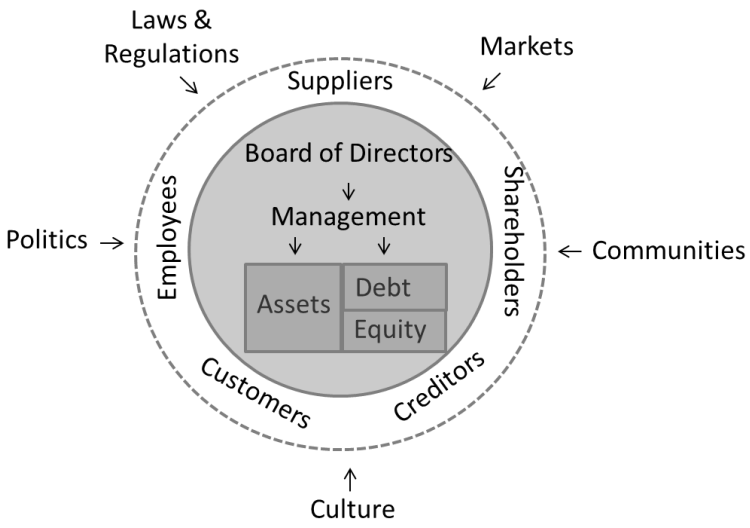

Figure 3: Corporate Governance adapted from Gillan (2006)

An overview of a firm and its corporate governance structures is displayed in Figure 3 (Gillan, 2006). Through this mechanism, policies and procedures are implemented for decision making, which have a direct impact on the stakeholders that keep a high interest in the firm's business activities. Examples of such stakeholders are the board of directors, management, shareholders, employees, etc. Corporate governance must set in place strong business principles, communicate corporate structures and dictate internal controls on how to reach the company's objectives. Due to the fact that shareholders appoint the executive board in public firms, the later must be held accountable to the shareholders in the event of poor performance and for erroneous disclosures.

The reasons why firms undergo initial public offering activities have been studied by academicians. Brau and Fawcett (2006) state that companies primarily decide to go public in order to simplify the process of future acquisitions. Pagano, Panetta and Zingales (1998) found that Italian traded companies have more bargaining power with banks compared to private firms, thus the cost for bank credit decreases. The researchers also affirm that public companies must employ externally certified accounts and that the firms are more visible to legal and tax authorities. This fact forces these organizations to establish responsible corporate governance.

In this regard, corporate governance targets the compliance to the principles of society. The compliance concept has different significances for each area where it is applied. In the fields of auditing and accounting, compliance is represented by the Sarbanes-Oxley (SOX) U.S. Act (SEC, 2002), in addition to improving the internal control system and the quality of financial reporting. SOX represents the most important law that affects organizations traded on the US stock markets, as stated by Gordon, Loeb, Lucyshyn and Sohail (2006). Gillan's (2006) corporate governance framework portrays SOX's importance, as observed in Figure 4.

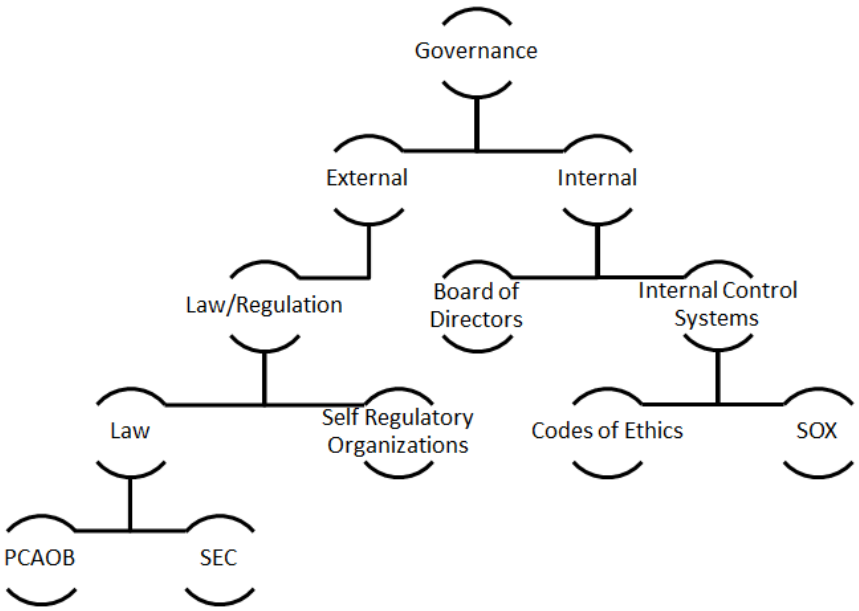

Figure 4: Corporate Governance framework adapted from Gillan (2006)

Currently, 27% of the 78,000 public companies that are registered on stock markets around the world[6] are listed in the US. This substantial portion of the world's publicly traded companies is required to comply with SOX. Moreover, another 28% of these firms are traded in countries that have enacted SOX equivalent laws. Although this number remains limited, i.e. in the Netherlands traded firms must conform to the Tabaksblat Code on a "comply-or-explain" principle (Akkermans, van Ees, Hermes, Hooghiemstra, Van der Laan, Postma, & van Witteloostuijn, 2007), and in Germany various mandatory and voluntary regulations have been enacted over the years (Goergen, Manjon & Renneboog, 2008), to the researcher's knowledge limited to no academic research has been performed in these regions. Consequently, due to the significant number of companies that must comply with SOX, this law is further described in this research.

The main motivator for the intensified attention on compliance in the accounting and control areas represents a chain of financial fraud scandals and bankruptcies in the US. Due to inefficient corporate governance, Chief Executive Officers (CEO), Chief Financial Officers (CFO) and Chairmen committed fraud by creating fictitious profits and concealing debts from their financial statements (Rezaee, 2005). The main reasons why public companies violated laws included a lack of management fraud, internal controls and fraudulent financial reporting (Rikhardsson, Best & Juhl-Christensen, 2006).

SOX was enacted by the U.S. government with the clear goal to strengthen the standards all U.S. publicly traded companies and public accounting firms must to adhere to. The rules included in the law are demanding and were designed to "*protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws*" (U.S. Congress, 2002). The SOX established new financial reporting accountabilities in order to certify the integrity of financial audit records.

[6] http://www.crmz.com/Directory/

Singleton (2003), and Kaarst-Brown and Kelly (2005) affirm that IS research was unsuccessful at recognizing the complete consequences of SOX and try to raise the awareness of the SOX's consequences on IT budgets, IT governance and relationships with software vendors and outsourcing companies. Hall and Liedtka (2007) argue that IT outsourcing should not be a first-choice decision when complying with SOX. The areas targeted by SOX, i.e. management accountability and operating efficiencies, are in a close relationship with IT (Kaarst-Brown & Kelly, 2005). Technology and systems are not the only areas SOX has a significant impact on other regions as depicted in Figure 5.

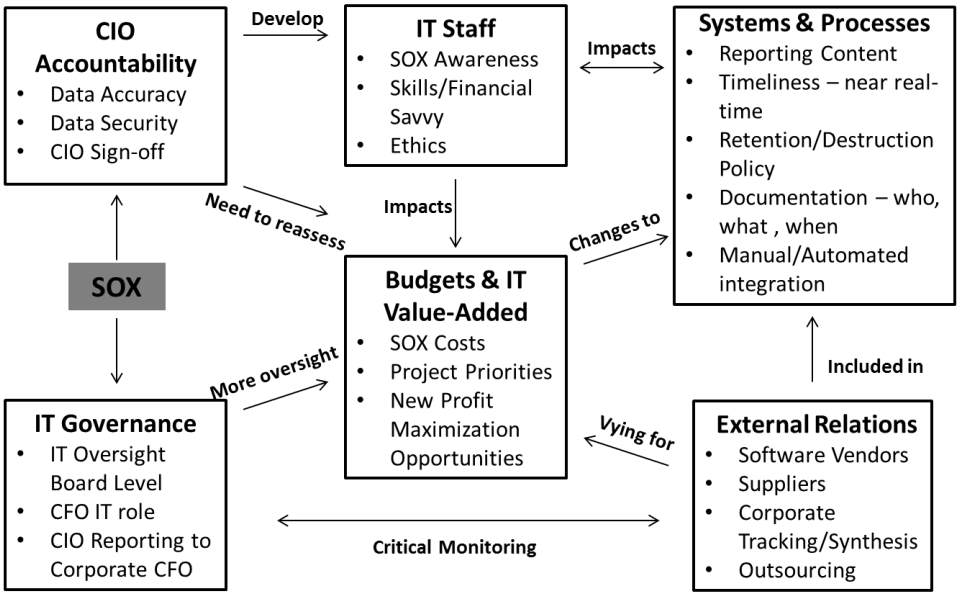

Figure 5: Impact of SOX adapted from Kaarst-Brown and Kelly (2005)

Consequently, Kaarst-Brown and Kelly (2005) urge academicians and practitioners to consider SOX as an examination of "organizational transformation, information systems integration, and IT functional adaptation". A strong internal control system built within IT can improve the IT governance, optimize operations by focusing on availability, security and integrity of processes and provide a competitive advantage due to the increased level of efficiency and effectiveness of operation (Fox & Zonneveld, 2003; Damianides, 2005; Debreceny, 2006).

According to Brown and Nasuti (2005), many issues exist in ERP applications. For example, change management and process reengineering pose medium to high threats to the financial information within an enterprise. As a consequence, regular risk management of the business processes is required by SOX and transforms ERP systems into a central accumulation point of an enterprise's risk management data. Brown and Nasuti (2005) believe that the frameworks established to meet the SOX requirements will provide the necessary capabilities for improvements to the IT environment.

Brown and Nasuti (2005) describe that sections 302, 404, 409 and 802 of SOX are directly connected to the IT landscape of a firm. Only Section 404 is of importance to this research because it explains the assessment criteria of internal controls. The shift from minor consideration of the internal controls to elaborate testing and examination has been put into

practice by Audit Standard No. 2, enacted by Public Company Accounting Oversight Board (PCAOB, 2004). This Standard together with Section 404 constitute an extensive change in the traded organization's internal controls (Brown & Nasuti, 2005) as both the management and a registered public accounting auditor are obliged to submit each one report at the end of every financial year (Morris, 2011).

The management's internal control report must contain (Brown & Nasuti, 2005):

- A declaration of their accountability for setting in place and continuously monitoring the framework of internal control over financial reporting (ICFR), in order to provide a reasonable assurance level of the financial disclosure.
- A disclosure of the procedures used in assessing the effectiveness of the ICFR. These procedures are assembled into a framework which SEC (2003) requires to be a "*suitable, recognized control framework".* The Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework is distinguished as a "suitable" architecture that helps public firms meet the requirements of the SOX act, as recognized by SEC (Gupta & Thomson, 2006).
- The evaluation of the execution of the internal controls which must be delivered at the end of the most recent fiscal year. Moreover, management must express the status of the evaluation of the ICFR.
- An appointed auditor to perform the financial statements. This auditor must provide also his/her opinion on the management's assessment of ICFR. This attestation must contain any intentional and unintentional errors in the case of insufficient controls.

3.2 Internal Control over Financial Reporting

Before SOX, standards related to corporate reporting were scarce (Doyle, Ge & McVay, 2007). Internal control over financial reporting has been identified, in prior academic research, as a significant characteristic of an organization (Kinney, 2000). ICFR refers to all the measures set in place by the management in order to provide a reasonable assurance of the company's financial state.[7] The existing guidance does not explicitly state what the boundaries of reasonable assurance are. Even though attempts have been made to narrow the gap between the expected level of assurance an audit reports must contain, and the level of

[7] ICFR is defined as "*those policies and procedures that: (1) Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements*" (PCAOB, 2004).

audit reports actually have[8], this concept is still mainly based on the auditor's professional opinion (PCAOB, 2004).

Moreover, reasonable assurance does not offer the same security as complete assurance. Regardless of the amount of effort invested into an internal control system, it will never reach complete assurance because it is prone to human errors and misjudgments, impossibility to inspect all evidence and the system's limitations. Prevention and detection status refers to the nature of the controls that are designed within an internal control system.

In order to fulfill the effectiveness of ICFR, no material weaknesses need to be present (PCAOB, 2004). A material weakness is defined "*as a significant deficiency that leads to a material misstatement of the annual or interim financial statements"*. A significant deficiency as a "*control deficiency […] that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles*".[9] Furthermore, a control deficiency exists when the control obstructs the personnel from timely preventing or detecting inaccuracies. This deficiencies spring either from the design of the control or its operation. The deficiency in design happens when there is a lack of a control that is supposed to fulfill the control objective or its design is flawed. The deficiency in operation arises from the mismatch between its design and its operation, or when the person in charge of its execution lacks the proper authorizations to execute it effectively.

Several studies (Ge, McVay, 2005; Ashbaugh-Skaife, Collins & Kinney, 2007) identify that the material weaknesses disclosed by public firms are related to inadequate revenue-recognition schemes, inadequate period-end close of reporting processes and accounting policies, improper account reconciliations and lack of segregation of duties. A positive correlation exists between material weaknesses and business complexity, i.e. foreign currencies and various market sectors. Doyle, Ge and McVay (2007) discover that weakness in ICFR are more likely to be found in young, small traded companies that are financially fragile, complex, are growing at a fast pace and are experiencing restructuring. Morris (2011) discovered that organizations that have an ERP solution in place are less likely to communicate material weakness than firms that do not run an ERP system.

The auditors that audit a firm's financial numbers have the objective "*to obtain reasonable assurance that no material weaknesses exist as of the date specified in management's assessment*" (PCAOB, 2004). The evaluation factors on which material weaknesses are identified must be both quantitative and qualitative. One example of qualitative factors represents the characteristics of the financial accounts and the potential outcomes of prospective deficiencies. In addition, the auditor must examine the consequences of compensating controls and whether they are sufficient. Organizations have established audit

[8] *http://www.nysscpa.org/cpajournal/2005/1105/special_issue/essentials/p28.htm*

[9] To the researcher's knowledge, all the scientific papers that were analyzed reference the above-stated definitions.

committees as a consequence of SOX. Additional research revealed that audit committee quality is positively associated with the internal control quality (Krishnan, 2005).

3.3 Internal Controls

3.3.1. Controls

SEC (2007) state that a control "*consist of a specific set of policies, procedures, and activities designed to meet an objective*". Controls can be implemented in specific parts or workflows within processes, and may be used with different perspectives. One perspective is their usage as decision making mechanisms to reach the established objectives. Another form would be to review and detect unusual behavior that emerges when trying to accomplish the company's ambitions. Finally, controls can be used to prevent possible future anomalies within the organization, steering it from its main goals. In this regard, controls are apparatus set in place by the management team of an organization at all its levels to monitor that operations are performed as intended.

The definition of internal controls, on the other hand, has evolved over time. Starreveld, de Mare and Joels (1994) refer to internal controls as set of rules, procedures. Controls are established to support and analyze business processes. Root (1998) states that the usage of this terminology was mainly observed in the accounting line of work, while Dassen, Maijoor and Wallage (2002) argue that it primarily deals with the integrity and quality of information systems. The interpretation that is standardly accepted by organizations worldwide is retrieved from COSO (1992): "*a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives*". These objectives are related to the efficiency and effectiveness of business activities, reliability of the financial reports and the compliance efforts (Damianides, 2005). The management leverages an organization's business activities when it possesses an efficient and effective internal control system. This should provide reasonable assurance the business is in control.

3.3.2. Internal control and organization

Internal control structures are set in place in order to reflect the reality in a truthful and correct manner. This means that the information that is distributed within the organization and to external parties must be reliable. Starreveld et al. (1994) argues that information is transmitted by means of systematically processing, collecting and storing all sorts of data. Due to the increased amount of data available, tools associated to information and communication technology field are employed to retain it. Large enterprises invest considerable amounts of money into information systems (Swartz, 2003; Carney, 2006), such as ERP systems or financial systems, in order to cope with the increasing complexity of business transactions. Additionally, the use of ERP environments and the use of non-financial performance indicators are considered to increase the corporate performance level (Wier, Hunton & HassabElnaby, 2007).

Moreover, one factor that determines the success of an ERP system is its effect on internal controls (Valipour, Moradi & Fatheh, 2012). The performance of business operations is being

measured by running all sorts of reports, including financial ones, within these enterprise systems. Consequently, a large percentage of the internal control measures are based on these applications. Like any software applications, automated internal controls lead to the rise of new enterprise-wide risks, which results in additional defensible approaches against new risks. These measures are strongly related to the general infrastructure of a technology system.

Basten (2004) categorizes controls into three groups: organizational controls, application controls and general IT controls, such as depicted in Figure 6.

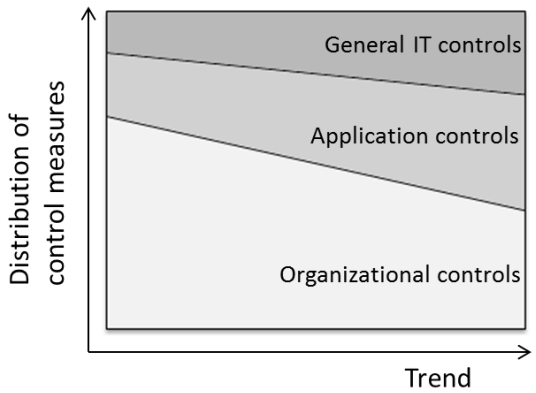

Figure 6: Scale of controls adapted from Basten (2004)

The organizational controls relate to the organization itself and reside outside the technology systems. A few examples are: organizational user separation of duties, physical access security, monitoring of system users based on reports. On the other hand, application controls are to be found at the opposite end, within the information systems. Such controls include: application user separation of duties, required mandatory fields (payments of goods are performed to vendors that have a bank account in the information system's master data), access security, system configuration, logging of user activities. The proper functioning of these internal controls is being managed by the general IT controls. Chan (2004) also mentions that security of assets and authorizations represent key organizational internal control objective and they belong to the IT-related objectives of establishing and maintaining information privacy, confidentiality and security.

Controls can be split into two categories: automated and manual (SEC, 2007). Manual controls refer to manual investigations completed by personnel and consist of inventory counting on a regular basis or a match between the amount of goods that were received by an organization and the amount stated on the invoice that is delivered with them. Automated controls on the other hand refer to the controls that are planted into the business activities and that sustain these activities in the enterprise system overflow (Rikhardsson, Best & Juhl-Christensen, 2006).

De Bruijn and op het Veld (2008) affirm that IT general controls contain both automated and manual elements. This set, IT general controls, encompasses IT dependent manual controls as well as IT application controls. Due to their absolute utilization in the enterprise system, IT

application controls are the exact opposite of manual controls. IT application controls are utilized by the system every time a transaction is being created and processed throughout the system. Such controls are segregation of duties, authorizations, purchase order approvals, etc. Additionally, de Bruijn and op het Veld (2008) mention IT-dependent manual controls as controls that contain both manual and automated characteristics. One specific example would be the print of a report over all the discounts for goods that were delivered late to the customers. The automated part is represented by the fields that need to be filled into the system to receive a report that contains the exact data that is wanted, whereas the manual part deals with the review that needs to be undertaken. A visual representation is provided in Figure 7 below.

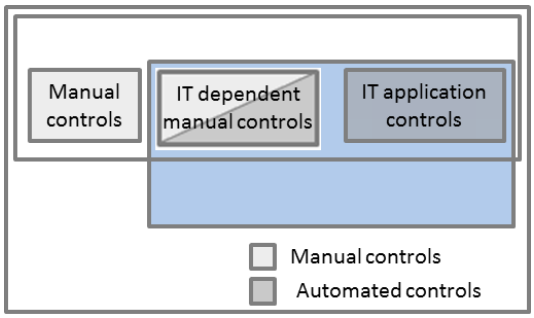

Figure 7: Business process internal controls classification adapted from de Bruijn and op het Veld (2008)

3.3.3. Control measures

The quality of data is being provided by control measures. If the right control measures are established and executed on a regular basis, then performance of operational processes can be measured. Organizations strive to set in place highly effective and efficient verification measures in order to be 'in control' of their business. From this point of view, Moeller (2005) categorizes controls as:

- Preventive controls: On one hand, these controls are essential in an internal control system as they assert the quality of enterprise systems. Preventive controls are proactive and form the first line of defense against erroneous manual inputs of data, as they prevent errors and inconsistencies from occurring. One example would be the set-up of segregation or separation of duties within business workflows.
- Detective controls: These controls, on the other hand, are meant to detect any errors and deviations from normal behavior after they have occurred. These anomalies manage to bypass the preventive controls within the system. An illustration would be the reconciliation of financial accounts.
- Corrective controls: This type of controls is used in parallel with the detective ones in order to recuperate from the losses and damages inflicted to the organization. One type of corrective control is an insurance policy to compensate for damages.

These three control techniques are essential aspects in any type of internal system control. Moeller (2005) argues that the implementation of preventive control techniques are most

cost-effective, while detective controls form a compulsory part of any system of control. Moreover, without any corrective actions detective controls bring little value. For example, internal audit operates as a detective control technique that concludes whether preventive controls function as intended. It is though the management's responsibility to employ the necessary corrective actions that will react to the identified control findings.

3.3.4. Internal control frameworks

Academic research has showed that, since SOX, several internal control frameworks have been developed to provide guidance on how to adhere to laws and regulations. A recognized and standard internal control framework for financial reporting is represented by the COSO Framework (COSO, 1992). In order to provide guidance for the IT security and control areas, Control Objectives for Information and related Technology (CobiT), a generally used and standardly accepted framework (Lainhart, 2000), has been developed. CobiT is regarded as a supplement to the COSO framework (Ramos, 2004) because the later does not consider the IT risks (Bonnie & Watson, 2009). Although Larsen, Pedersen and Andersen (2006) create a complete overview of specific internal control frameworks, Tuttle and Vandervelde (2007) advocate that "*no practitioner developed internal control framework has undergone rigorous academic examination in the same manner that researchers routinely examine the conceptual models developed by other academics*". Tuttle and Vandervelde's (2007) study regards CobiT as a useful mechanism for financial statement audits, but also compliance and operational audits. Due to the fact that the majority of organizations are using the COSO framework as a general framework for their assessments and that the rest of the frameworks are specifically-tailored frameworks, the COSO framework will be further explained. Moreover, Valipour et al. (2012) conducted a survey in a company that was using an ERP system in their day-to-day operations and found that the firm's five components of the COSO framework have considerably improved after adopting the enterprise solution than firms that are not using such a system.

COSO was established with the main goal of improving the critical aspects of risk management, internal control, financial reporting and fraud (Simmons, 1997). The Framework contains guidelines and general steps on the design, implementation and assessment of internal control mechanisms in any type of organizations. Organizations have rather complex control procedures and that some business units function in highly structured environments with highly structured control workflows while other operate in less formal processes (Moeller, 2005). COSO modeled a three-dimensional cube to describe an internal control system. This cube is depicted in Figure 8.

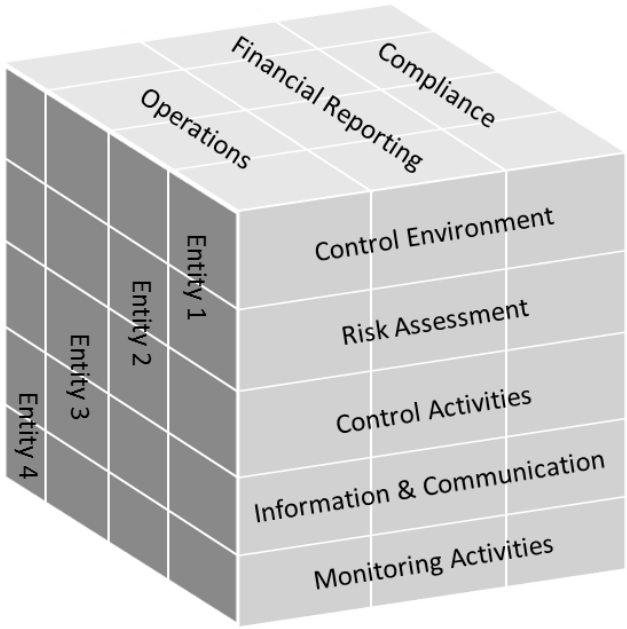

Figure 8: Relationship of Objectives, Components and Entities adapted from COSO (1992)

The framework identifies the relationship between the different elements: objectives, components and entities. These are to be found in an internal control system. Based on the mission statement and the vision of an organization, the management established objectives. On the upper side of the cube three objectives are identified: operations, financial reporting and compliance. Operational objectives concern all the efforts carried out at an entity-level, i.e. subsidiaries, business units, etc., in order to reach the enterprise-wide goal. Financial reporting objectives are linked to both internal and external disclosure of company financial figures. Compliance objectives deal with the conformity to laws and regulations imposed by market regulators.

The five components of an internal control environment are: Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring Activities. The first component represents the essence of the rest of the components. The control environment is established by the executive board in a top-down approach, such that it sets the significance of a control system and the norms and standards that come with it. For every objective there are a multitude of risks. These risks should be identified and assessed, and a clear view on how they should be managed should be constructed. This is included in the Risk Assessment component. The Control Activities area deals primarily with the internal policies that the management establishes with the scope of reducing the risks are literally followed by the personnel. These control activities are included in every corner of the organizations businesses. Information is exchanged throughout the entire company to reach the established targets. Communication is present both internally, i.e. staff is aware of the internal control activities, and externally, i.e. reporting to the organization's stakeholders. The final component, Monitoring Activities, deals with all sorts of evaluations within the organization to determine whether all components are in place and function as intended. In the event of malfunctioning, issues are revealed to the management and the executive board.

On the side of the cube, various entities are identified as organizational departments such as functions, operating units, entity levels and divisions (COSO, 1992).

3.4 IT Control Measures

Fox and Zonneveld (2006) state that regardless of the market sector organizations operate in, all sectors contain risks. Compliance to governmental laws and external regulations, SOX in particular, does not secure risk-free conditions, but it does make organizations more aware of their exposure and it clearly brings a number of benefits. Benefits that are worth mentioning are: competitive advantage, increase level of efficiency and effectiveness of operations, increased level of IT governance, better quality and timely information.

According to Fox and Zonneveld (2006), controls within organizations are to be found at three different levels: Executive Management, Business Processes and IT Services. These common components of companies are illustrated in Figure 9.

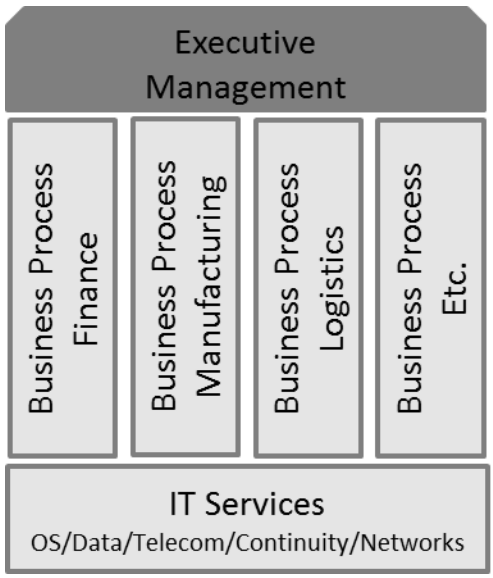

Figure 9: Common elements of organizations adapted from Fox and Zonneveld (2006)

As explained in the Control Environment component of the COSO Framework, executive management combines the business strategy with business activities. The executives set the tone on what policies need to be followed and how resources are to be utilized in order to reach the business objectives. Some of the controls included, originating from this area are: internal audit, procedures and policies, quality assurance, plans and strategies, risk assessment, and education and training. The Business Process element refers to the manner by which organizations deliver value to its stakeholders. Part of the business processes are inputs, processing and outputs. As a natural trend, business workflows are automated to a highly degree, thus they are embodied in complex IT systems. Application controls are part of the Business Process element and the control objectives comprise of disclosure of data, authorizations, accuracy and completeness of data. Operations are based on IT systems. These systems provide for the organization as a unity and not for specific branches within the organizations. Such IT services are managed by a central IT department and often include

storage, operating systems, databases, network management and application management. Furthermore, examples of controls in the IT Services area, entitled IT General Controls by Fox and Zonneveld (2006), include program development and changes, computer operations, and access to program and data.

The nature of these groups of controls is the same as the one Basten (2004) mentions. Due to the fact that the current research project focuses on the controls that are within information systems, only application controls and general IT controls will be treated in a detailed manner in this thesis, excluding the organizational control measures. A more detail explanation is given in Section 3.6. General IT controls often support the application controls. Application controls are integrated in the IT applications and help various business units in their day-to-day processes, thus they are located in ERP, Customer Relationship Management (CRM) and Supply Chain Management (SCM) systems.

A way of further dividing General IT and application controls is presented in Table 6 and described in the subsequent subchapters.

Table 6: IT Controls classification

IT Control Measures	Mentioned by
General IT Controls Groups	
Change management	Fox & Zonneveld (2006); Senft & Gallegos (2009)
Physical security	Fox & Zonneveld (2006); Senft & Gallegos (2009)
Logical security	Fox & Zonneveld (2006); Senft & Gallegos (2009)
Segregation of duties	Fox & Zonneveld (2006); Senft & Gallegos (2009)
System development	Fox & Zonneveld (2006); Senft & Gallegos (2009)
System administration	Fox & Zonneveld (2006); Senft & Gallegos (2009)
Interoperability controls	Senft & Gallegos (2009)
Application Controls Groups	
Input controls	Fox & Zonneveld (2006); Senft & Gallegos (2009)
Processing controls	Fox & Zonneveld (2006); Senft & Gallegos (2009)
Output controls	Fox & Zonneveld (2006); Senft & Gallegos (2009)
Data communications	Senft & Gallegos (2009)

3.4.1. General IT control measures

Change management

As expressed by Basten (2004), the proper functioning of application control measures is being managed by the General IT controls. Change management process is strongly related to this group of controls because whenever a change is performed on an activity that executes an identifiable and distinct task, then that alteration might lead to business losses. Thus its main purpose is to decrease the number of errors and disruptions that are related to an information-processing environment (Senft & Gallegos, 2009). As mentioned before, multi-national companies have very complex IT infrastructures that rely on elaborate software, hardware

and applications that are interconnected. As a consequence, every time a change is proposed, Senft and Gallegos (2009) affirm, it needs to clearly be defined, planned, coordinated, tested and implemented, following the same path as software requirements. Change management relates to the internal policies, rules and tactics created by the upper management, in order to be able to evaluate whether the objectives contained in the information strategy are realized.

Physical security

Physical security deals with the prevention, detection and minimization of unauthorized access, damage and theft of network-related supplies and all sorts of devices pertaining to the technical infrastructure. A few examples include: prevent unauthorized personnel to enter the server space by introducing an electronic lock on the door, prevent the theft of company-sensitive data by hiring security guards and installing alarms.

Logical security

Assembled from the ISO/IEC 27002 (2005) standard, logical security is part of an organization's information security policy and depicted in Figure 10.

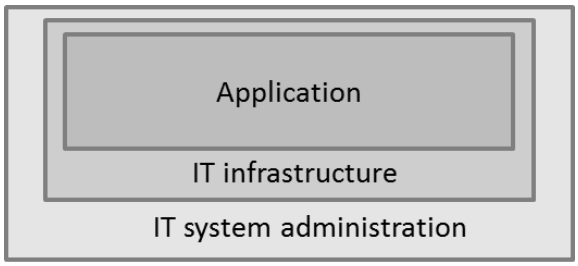

Figure 10: Logical security

The logical security is composed of three levels: application security access, IT infrastructure security and IT system administration security. The degree of security of each of these components states whether an IT environment is secure or not. Application security contains all the measures within system applications, i.e. user profiles, roles and rights. The IT infrastructure security sets all the security measures of the enterprise-wide IT system and it does not address individual tasks, functions, or applications. Examples of IT infrastructure security actions are network access, database systems, operating system, etc. In order for a user to access the data warehouse, he/she must be provided with the adequate access rights. This is the reason why application security is built within IT infrastructure security. IT system administration security deals with the administration of the IT infrastructure, i.e. the monitoring of security sections, access requests, assigning user profiles, maintaining user accounts, etc.

Segregation of duties

COSO (2011) define segregation of duties (SOD) as the policy of separating different responsibilities among different staff members for recording, authorizing and approving various transactions within business processes and handling company's assets. For example, losses can occur due to fraudulent activities if the same user can create a fictitious purchase order (PO), record a high-valued PO within the enterprise system and approve the payment.

Moreover, SOD covers also managerial overrides, and represents a significant threat, i.e. fraud, if no strict internal policies are in place to regulate the division of duties.

System development

As organizations make extensive use of ERP systems to cope with the complexity of their business processes, enterprise system development and system maintenance controls play an important and supporting role in the success of an organization. These controls assess the quality level of system development methodology and future post implementation requirements, i.e. extensions to the existing system capabilities, (Senft & Gallegos, 2009).

System administration

Senft & Gallegos (2009) state that managing an IT system constitutes a critical component in distributed open systems. Even though standard implementations exist, many companies opt to tailor large-scale systems to match their own business processes. As a result, many risks arise, and the complexity of administering such a system, or a multitude of different software products from multiple vendors increases. Such controls include checks on number of authorized licenses and the ones used, monitoring system performance and checks on whether networks printers are working properly.

Interoperability controls

This type of controls refers to data conversion and data adjustment techniques (Senft & Gallegos, 2009). Data modifications occur when new ERP systems are implemented and data must be captured from old (legacy) systems. Therefore, controls are designed to monitor if all the data is transferred into the new environment and whether the transferred data is accurate enough. Senft and Gallegos (2009) also cover the controls over interfaces. On one hand, these controls relate to the aspect users input information into the ERP system and, on the other hand, the way the new ERP system is integrated with other legacy systems and the flow of data between all the environments.

3.4.2. Application control measures

Application controls are a component part of the transactional system (Basten, 2004; de Bruijn & op het Veld, 2008; Fox & Zonneveld, 2006). Every time a user inputs data into the system, a business process is executed throughout the system, leading to an output of data. Senft and Gallegos (2009) state that application control measures are intended to safeguard the completeness and consistency of transactions. The measures include screen edits, running checks against predefined rules or numbers and expected volumes, reconciliations among systems, etc.

Input controls

Such controls are introduced to lower the risks that might occur when data is being entered into the system (Senft & Gallegos, 2009). The consistency, timeliness, completeness and authenticity of data input, both manually and through automation, are guaranteed by input controls. Their main tasks are to restrict users/systems from recording defective transactions and avoid valid transactions that contain inaccurate data. This is managed by limiting the access to the screen, selecting an authorization user on transactions above a certain threshold,

validating the data input before processing the transactions, establishing error-handling mechanisms, and monitoring business transactions on a timely basis.

Processing controls

Senft and Gallegos (2009) explain that processing controls are critical controls to the overall health level of a system as they are used to ensure the consistency, timeliness, and completeness of data during a whole cluster or real-time processing. Critical risks appear if data is not accurately processed, such as loss of data or capturing unreliable data. The same verification techniques are performed to verify the reliability of data as input controls: edit checks, validation checks, etc. Here, an exception report can be executed to output all errors and strange behavior within the system, report which is sent to the process owner for review.

Output controls

Accurate and timely information leads to better decision making. Output controls make certain that the output is complete, correctly generated and received in a timely manner (Senft & Gallegos, 2009). One example of output control covers the procedures for the delivery of reports, either paper-based or electronic form.

Data communications

Data communications controls are mainly oriented toward transmission controls (Senft & Gallegos, 2009). These controls are set in place to restore and protect data from undesired errors. Such errors cover long distances, the speed with which data is transmitted over the wires, or equipment failure.

3.5 Continuous Auditing

The academic literature identifies two types of audits: internal and external. The internal audit was primarily based on detecting material weaknesses prior to SOX (Hass, Abdolmohammadi & Burnaby, 2006). After SOX, the internal audit's function shifted from a controls approach to a risk-based attitude. Another noticeable change is represented by the fact that internal auditors are required to participate in the creation of control documentation and compliance auditing over financial reporting, duties pertaining to the external auditors by that time. The internal auditors's coverage adjusted to being involved in the design and execution of internal control systems. Hass, Abdolmohammadi, Burnaby (2006) mention that in the first year of SOX more than half of the internal audit team in every publicly traded US company was involved in the SOX assurance endeavors, leading to a decrease in resource allocation for operational audits. One facilitator for SOX compliance represents Continuous Auditing (Vasarhelyi, Alles, Kuenkaikaew & Littley, 2012).

Over the years, audit has evolved from manual to system-based techniques (Groomer & Murthy, 1989; Rezaee, Elam, & Sharbatoghlie, 2002; Vasarhelyi, Alles & Kogan, 2004). The research area of continuous auditing (CA) was initially proposed by Kogan, Sudit and Vasarhelyi (1999). CA is defined by Alles, Kogan and Vasarhelyi (2002) as the application of technological capabilities to the standard audit efforts, both external and internal, on a regular basis. The concepts of continuous monitoring and continuous auditing are used with

the same meaning in the scientific body of knowledge, as they refer to the examination of real-time data by using pre-determined rules (Kuhn & Sutton, 2010). Even so, a difference between the two has been observed, namely CM is a management's duty and CA is an auditor's responsibility (Warren & Parker, 2003; Henrickson, 2009). Moreover, Alles et al. (2008b) observe that CA overlaps with operational monitoring set in place by the management, defining CA as a subset of Continuous Management Monitoring (CMM). CA is driven by the reporting element, entitles Continuous Reporting (CR) (Rezaee & Hoffman, 2001; Nehmer 2003). Kuhn and Sutton (2010) define this term as a reporting capability based on predefined criteria and, in a CA context, as a capability that distributes alerts triggered by violations of controls. At the macro level, CA is positioned as a subset of Continuous Assurance (Alles et al., 2002; Kneer, 2003).

Based on the rich body of scientific knowledge on CA, Brown, Wong and Baldwin (2006) have identified a number of demand factors for CA: the need to disclose information more frequently to better help decision makers (Elliott, 2002; Hunton, Wright & Wright, 2002; Rezaee et al., 2002); the rapid growth of the electronic environment (Kogan et al., 1999); more timely detection of irregularities (Vasarhelyi, Kogan & Alles, 2002); the need to ascertain that business transactions operate as intended (Greenstein & Ray, 2002; Vasarhelyi et al., 2004); enterprise and data warehouse environments (Rezaee et al., 2002; Vasarhelyi et al., 2004); SOX (White, 2005); and the electronization of the business environment (Vasarhelyi & Greenstein, 2003).

A number of guidance theories, frameworks, techniques and audit maturity models have been developed over the years to fill a gap in the continuous auditing domain (Groomer & Murthy, 1989; Woodroof & Searcy, 2001a; Borthick, Jones & Kim, 2001; Chen, 2003; Chen, 2004; Murthy, 2004; Zhao, Yen & Chang, 2004; Dull, Tegarden & Schleifer, 2006; Kuhn & Sutton, 2006; Li Huang & Lin, 2007; Vasarhelyi, Kuenkaikaew, Littley & Williams, 2008; Teeter, Alles & Vasarhelyi, 2010; Chan & Vasarhelyi, 2011). Vasarhelyi et al. (2004) identify four levels of analysis during an audit and assemble a hierarchy of audit processes based on their relationship with the control activities. Rezaee et al. (2002) provide an approach that combine audit data users, audit data servers and data sources. Due to the high academic interest, research has been undertaken to compare some of the existing continuous auditing tools and techniques (Flowerday, Blundell & Von Solms, 2006). Due to a strong interest between academia and industry, a number of methods were also applied in real-time systems (Vasarhelyi & Halper, 1991; Rose & Hirte, 1996; Murthy, 2004; Nelson, 2004; Turoff, Chumer, Hiltz, Klashner, Alles, Vasarhelyi & Kogan, 2004; Pathak, Chaouch & Sriram, 2005; Alles et al., 2006; Coderre, 2006; Li, Huang & Lin, 2007; Alles et al., 2008).

Regardless of the method used, CA is regarded as a cost-effective assurance mechanism (Brown et al., 2006). In this regard, researchers have identified, from an audit's perspective, a series of benefits that lead to positive behavioral impacts (Hunton et al., 2002); decreased cost of capital (Elliott, 2002); decreased audit risk (Rezaee et al., 2002); increased efficiency and effectiveness of the audit (Searcy & Woodroof, 2003a); decreased compliance costs (Woodroof & Searcy, 2001b; Rezaee et al., 2002; Searchy & Woodroof, 2003; Pathak et al., 2005; Hunt & Jackson, 2010); timely delivery of information to decision makers (Nehmer,

2003); shorter audit cycles (Nehmer, 2003); increased probability that material errors and fraud may be revealed (Chan & Vasarhelyi, 2011); execute operation tests (i.e. duplicate payments) to assess whether those controls perform as intended (Vasarhelyi, 2004); identify areas for improvements (Chen, 2003); decreased number of errors and mistakes that occur during an audit (Chen, 2003); increased level of data integrity and reliability (Vasarhelyi, 2004; Zhao et al., 2004); increased sample size or population (Rezaee et al., 2002; Vasarhelyi, 2004; Chan & Vasarhelyi, 2011); an increased audit quality (Rezaee, 2000); decreased costs for assuring compliance (Pathak et al., 2005); evidence of all audit findings and assertions (Rezaee, 2000; Rezaee et al., 2002; Alles et al., 2009); labor cost savings (Alles et al., 2006) and lower audit fees (Chen, 2003); shift of the auditor from performing tedious manual work to tasks that require examinations of exceptions (Chan & Vasarhelyi, 2011), and organizations will be better prepared for an audit (Chen, 2003).

Additionally, a number of challenges when adopting CA have been identified by the scientific world. The need for IT trained staff and high levels of trust between organizations and external auditors are mentioned as major challenges (Chen, 2003; Searcy et al, 2003b; Kuhn & Sutton, 2010). Searcy et al. (2003b) also state that the need for improvement of controls is an impediment for CA. Flowerday et al. (2006) mention that various sources, including legacy systems, and data formats pose a real challenge to CA. Handscombe (2007) argues that CA requires management support in terms of permission rights for external auditors to access data. Hall and Khan (2003) insufficient IT knowledge in the audit department might slow down the adoption rate. Taylor and Murphy (2004) suggest that the initial and ongoing costs of CA will hinder its adoption. Alles et al. (2006) mention that the reengineering of audit processes will be necessary when adopting CA.

3.6 Continuous Monitoring

For this section a combination of scientific literature, three semi-structure interviews and multiple unstructured interviews and discussions were carried out. The literature study educates the reader on the terminology. The unstructured interviews and discussions were performed for a period of 7 months with practitioners within BWise, in order to obtain in-depth information about their CM solution and identify the statements of the questionnaire. The semi-structured interviews (the last three rows of Table 7) provided information on the perceived benefits of CM and the challenges that one organization might face when considering a CM solution. These challenges and the ones identified in the previous section are compared to the challenges mentioned by the respondents of the questionnaire in Section 4.2. An overview of the experts involved can be observed in Table 7.

Table 7: Experts overview

Respondent type	Sector	Category	Size FTE
Product Owner	Technology	Computer Software	100-200
Developer	Technology	Computer Software	100-200
Developer	Technology	Computer Software	100-200
Tester	Technology	Computer Software	100-200
Architect	Technology	Computer Software	100-200
R&D Manager	Technology	Computer Software	100-200
CTO/Founder	Technology	Computer Software	100-200
Compliance Leader	Technology	Manufacturing	30,000+
Head of Financial Control	Technology	Medical equipment & Supplies Manufacturing	1,000 – 5,000
External Financial Controller	Consultancy	Audit	100,000+

3.6.1. Theoretical background

Continuous Monitoring (CM) has its roots in the corporate governance, financial reporting and auditing domains. Although CM has emerged with an identical meaning as CA (Kuhn & Sutton, 2010), a clear delimitation started to be observed over the past years between CM and CA (ISACA, 2002; Warren & Parker, 2003; Daigle et al. 2008; Henrickson, 2009). CA has been divided into Continuous Control Monitoring (CCM) and Continuous Data Assurance (CDA) (Alles et al., 2006, 2008b; Alles et al., 2008a). While CCM contains techniques for monitoring access control and authorizations, system configuration and business process settings, CDA examines master data, transactions and key process indicators that make use of computer-based analytical techniques. Alles et al. (2009) identify that in the industry the term *continuous control**s** monitoring* frequently refers to a CM solution, but that concept should instead be categorized as CDA due to its functionalities. Murthy (2004) uses the terminology of Continuous Monitoring Controls to refer to the same idea. Teeter and Brennan (2008) argue that automated continuous monitoring tools provide the means for *continuous control**s** monitoring* which is defined as the *"process of evaluating the effectiveness of internal controls in detecting errors and anomalies on an ongoing basis"*. Various methodologies have been developed and put into practice in order to undergo validity examinations (Groomer & Murthy, 2003; Huffman & Grump, 2005; Alles et al., 2006; Alles et al. 2008b; Nigrini & Johnson, 2008).

As explained in Section 3.5, various interpretations of the terminology exist in the academic literature as no standard definition is largely accepted, thus causing confusion. In line with Warren and Parker (2003) and Henrickson (2009), CICA/AICPA (1999) provide a general terminology in this field by defining Continuous Monitoring as *"a process to ensure that policies and processes are operating efficiently and to assess adequacy and effectiveness of controls".* Hunt and Jackson (2010) define Continuous Controls Monitoring as "*a technology*

solution for continuous monitoring which provides users with real-time status assurances for all of their compliance control points". In order to avoid confusion, one single terminology that comprises the two mentioned definitions will be used for CM.

Although no generally accepted terminology exists, several benefits of CM have been identified, such as lower audit costs; improving audit confidence (Gartner, 2009); lowering the risk of business losses due to timely reporting of misbehavior; removing redundant testing; improvements to the control framework by automating manual controls (Hunt & Jackson, 2010); improving operational performance to controls that test processes that might lead to losses, i.e. duplicate payments, and readily availability of control assessments and documentation (Gartner, 2009; Hunt & Jackson, 2010).

3.6.2. Practical example

Hunt and Jackson (2010) identify that CM is applied in four different critical areas of enterprise or financial systems. These areas are the Segregation of Duties, Application Configuration (AC), Master Data (MD) and Business Transactions (BT).

Continuous Monitoring of Segregation of Duties assesses whether all authorization measures within the IT system are in place and that no conflict of duties exist that might result in fraudulent activities (Boccasam & Kapoor, 2003). Continuous Monitoring of Application Configuration or application controls evaluates if the application measures that include screen edits, running checks against predefined rules or numbers and expected volumes, reconciliations among systems, tolerance thresholds of invoices, etc. operate as designed.

Continuous Monitoring of Master Data covers the monitoring process of system changes related to customers, products, currency rates, suppliers, vendors, employees, materials. For example, if the ratio between two currencies is inaccurate or there are duplicate entries for the same two currencies, then future decision-makers would be provided with inaccurate numbers regarding the sales amounts in those regions. Another example consists of changes to the base price of the products or materials. If the quality of those items is poor, then they would be sold at a lower price to customers or bought at a higher amount from suppliers. This area is important because reporting is executed dependently on master data, and any inconsistency leads to inaccurate business reports causing poor business decisions. Lastly, Continuous Monitoring of Business Transactions focuses on monitoring key financial processes such as Purchase and Payables (Potla, 2003; Coderre, 2006), Revenue and Receivables, Travel and Expense, etc. In order to understand the capabilities of a CM solution, a detailed example containing the risks and controls in the Purchase and Payables cycle (Figure 11) is presented based on interviews with practitioners from BWise.

In order to educate the reader, a simplified example is detailed. The Purchase and Payables process contains six sub-processes. In the Requisition stage, a user within the organization initiates the process by submitting a purchase request to a certain department. After the request is approved, an authorized user creates a purchase order and the order is submitted to the supplier. After a while, the supplier sends the goods and an invoice to the organization that ordered the goods. Next, the invoice and the purchase order are submitted to an

authorized user, i.e. financial accountant, and all the details are recorded in the enterprise system, after which the payment is made to the supplier's details by the enterprise system from the master database. Several risks and controls that can mitigate those risks can be identified. One risk is represented by a mismatch between what was ordered and what was received (BT). The control that would mitigate this risk would be the three-way match, which checks whether every invoice is referenced to a purchase order and the quantity of goods ordered matches the amount on the invoice and the count of the goods at their arrival. Limits and threshold are being set on the amount of over- and under-delivery for every region where the organization has subsidiaries, but if the tolerance setting is disabled or the tolerances are missing altogether, then this represents a configuration risk (AC). The entire process becomes even more complex when different regions have their specific limits and currencies. Due to significant volumes of transactions, payments can be made to duplicate invoices that are non-purchase (thus no purchase order is present) (MD) which would lead to a decrease in capital. Moreover, the payment must be in agreement with the invoice (BT) otherwise fraud can be committed. Poor quality of sensitive data of a supplier's bank account creates the risk of not making payments on time to that supplier, resulting in a halt of supplies until the error is identified and solved (MD). If a user is authorized to record an invoice or modify the amount of the payment and, at the same time, to change the bank account of the supplier on the invoice, then fraud can be committed. That user can transfer to his own account a one-time significant or multiple smaller amounts of money (SOD).

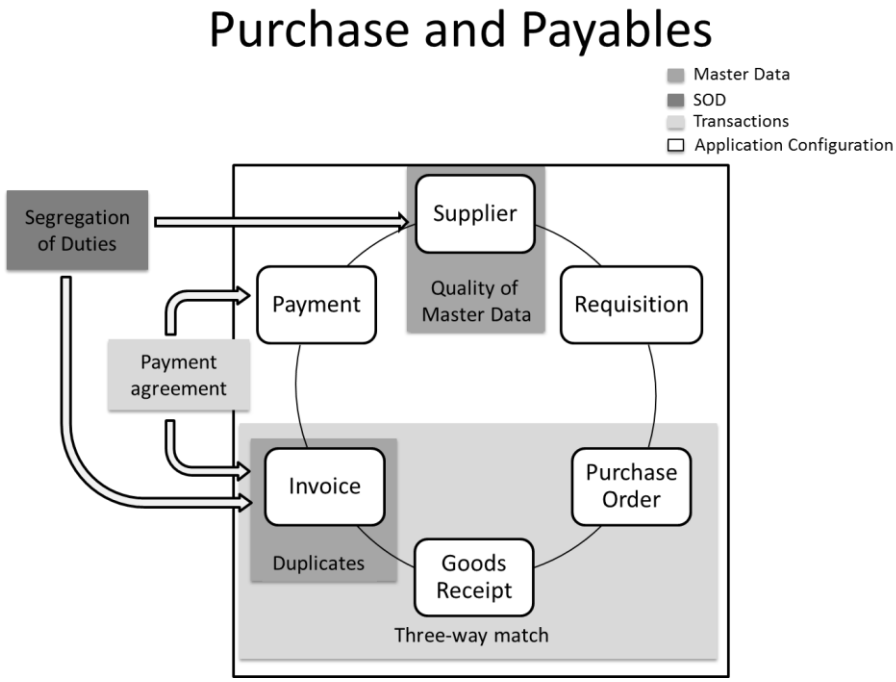

Figure 11: Purchase and Payables cycle

3.6.3. Problem and solution

Although companies have increased their efforts in automating their internal controls, manual controls still exist to a large extent (Hunt & Jackson, 2010). Enterprise systems are built so that the three-way match is correctly set and tolerance settings are appropriately set in place.

In spite of this, reports are being manually run at the end of the month to output incorrect matches and any exceptions are manually examined and corrected. Controls that require certain authorizations when a specific order above a predetermined amount has been placed are purely manual and are applied on a 'every time it happens' basis. Other controls tend to be automated and do not require any further human actions.

Hunt and Jackson (2010) state that companies do not have the means to assess the effectiveness of their internal controls system on a continuous basis and that they depend to a large extent on external audits to signal any inconsistencies. As a result, corrective actions are not exercised in an adequate timeframe that would avoid the issues identified in the auditor's internal control evaluation.

Based on interviews with practitioners from BWise and observed by Hunt and Jackson (2010) as well, a solution to this problem is the use of CM. In practice, Continuous Monitoring serves as a software tool that alerts business controllers, as frequent as they want to, whenever misappropriate behavior within the ERP or financial system is encountered.

A CM software solution assists control owners in their day-to-day activities by signaling in a timely manner if a control test resulted as ineffective, i.e. in the SOD, AC, MD, BT areas. To be more precise, rules are developed and linked to the internal controls within the Internal Control Matrix of an organization. A rule is linked to a control, i.e. three-way match. Every time the rule is trigger, a data analysis process occurs on the entire population of transactions within the ERP system, and an alert is submitted to the control owner responsible for monitoring the control. Exceptions are flagged, the analysis results are saved as electronic evidence and the control owner is informed in order to review the results and act in an appropriate manner.

The control owner is not required to actively test the control anymore, as he/she is alerted only when exceptions occur. Moreover, the analysis is based on examining the entire data set instead of selecting a small and random sample of transactions and performing manual matching. Part of the business responsibility is to assign certain limits and thresholds to rules. Reviewing every three-way mismatch might become labor-intensive if a large amount of exceptions are identified. If only the mismatches that are above a certain purchase amount and impact the financial statements on a high level, the reviewer focuses his/her attention on the activities that bring most value to the organization.

In order to assure that internal controls operate as designed, periodic checks must be performed by the control owners, known as control evaluation. Due to high costs, intensive manual work and increased amount of time needed to test the effective execution of a control, it has become the responsibility of internal and external auditors to perform it rather than the business owners (Hunt & Jackson, 2010). Audit reviews still represent a burden for control owners as they need to provide evidence and reports required by the auditors. Additionally, auditors only select a sample set of data and test it for validity.

Sampling represents the application of audit procedures on less than the entire population that is in scope of the audit. This limited amount disregards potential exceptions that might reside

in the untested part of the data set, creating a sampling risk (Hunt & Jackson, 2010) and causing misinterpretation of evidence. Continuous Monitoring eliminates the sampling risk as long as the data that is in scope of the audit resides in the ERP or financial system, thus it can only be applied to automated and semi-automated controls.

CM supports trending over time, audit analysis, notifications, alerts, reviews and approvals, all of which offer the necessary evidence for an audit trail. This software solution eliminates the need of sampling during the evaluations performed by the internal audit teams, and provides them with documented proof whether internal policies are followed in an appropriate manner and exceptions are documented properly. One example would be false-positives. They are exceptions that have a logical meaning or can be explained by the business owners. Without any evidence, the auditor must discuss the findings with them before finalizing their report. Continuous Monitoring is used as a central warehouse that contains all the results of the controls operation and testing (Hunt & Jackson, 2010).

3.6.4. Expert interview findings

Three semi-structured interviews with experts from the fields of Internal Control, Internal Audit and External Audit were performed with the scope to identify the stakeholders, the benefits and challenges of CM. The first finding was that all the interviewees stated that they see benefits from using CM technology.

From a business/controller perspective, several gain areas, which were not mentioned by researchers, were specified. To begin with, controllership management might benefit from CM by ensuring that staff does not have to examine the entire sample or population of transactions, but only the exceptions. It is critical that those exceptions are followed-up in a timely basis. In this way the awareness level and the data quality are increased. Moreover, the controller focusses on the risk areas that are less automated and require judgment. Unauthorized access is also a sensitive issue within the security of an enterprise system. Without the proper settings in place and without testing them regularly undetected fraud can take place. CM can help mitigate that risk. Another benefit would be the fact that CM produces evidence of the tests performed. This evidence is the controller's proof required by the auditor that he/she is in control of the business. This could lead to a lower stress level.

From an internal audit point of view, a few benefits that are not mentioned in the scientific knowledge have been stated by the interviewee. One benefit of CM would be the decreased amount of time spent on testing automated controls and increased amount on examining purely manual controls that require significant effort, i.e. spreadsheets that contain pricing and forecasting models. A real-time monitoring tool would also ensure a decreased degree of non-compliance probability, due to the fact that any issues within the system would alert the users in a timely manner and reliable reports would be produced. Furthermore, the interviewee specified that CM would also lower the time needed for travelling due to the electronic evidence that is produced in the system, making it unnecessary for the auditor to travel to remote regions to collect evidence. Kogan et al. (1999) have posed a research issue on the difference between the cost of implementing auditing systems and cost savings, i.e.

travel time. Consequently, this functionality would lower the stress level during an external audit.

From an external audit perspective, a number of gains related to CM adoption were identified. Firstly, the probability of future litigations should decrease, now that the business owners and the internal auditors are collaborating on a regular basis and not several times per year. This would also lead to an increased degree of reliability of the external auditor's yearly report. Due to the audit trail that a CM solution would record, the traveling time and testing time of controls are expected to decrease. The interviewer mentions that CM would add the testing of the rule as a necessary task in order to assess the overall reliability of the internal control. Although it does not happen that frequently, the participant stated that probability of racing the end-year audit in order to meet the deadline should decrease. As a final remark, CM should prove to be, in the long run, a matching tool for increased business complexity.

The interviewees also recognized a number of challenges, different than the CA challenges, that organizations would encounter when adopting CM. The main challenge toward CM is represented by the multitude of ERP, financial and legacy systems within organizations. Every platform has its own set-ups, slightly different controls, hence without an IT-centralized system, it becomes were difficult to extract accurate data. There was a common agreement that, when trying to implement CM globally, change management represent a significant issue. This is due to the fact that certain regions are more open for change than others. A solution to this problem, as suggested, is to implement CM locally, i.e. business unit, country, region, and then expand.

Chapter 4 Online Questionnaire

The research sub-question RSQ2 was answered by the means of an online questionnaire. Many advantages exist over traditional questionnaire such as functionality, flexibility and usability (Bandilla, Bosnjak & Altdorfer, 2003). Online questionnaires represent an excellent research technique as it may cover respondents regardless of their geographical location. Additional examples consist of the possibility of adding extra instructions per statement and of including skip patterns that appear invisible to certain respondents. The content of the online questionnaire was assembled based on the findings of the literature study on CA and CM, and expert interviews, as explained in Section 4.1. The answer to sub-question RSQ3 was addressed by comparing the challenges revealed by the literature study on CA and interview findings on CM, with the ones captured by the questionnaire. The results of the questionnaire are to be found in Section 4.2.

4.1 Online Questionnaire Setup

A scientific approach was adopted for the identification of the possible benefits that CM delivers. The content of the online questionnaire was assembled based on the findings of the literature study on CA and CM, and three expert interviews in order to assure its completeness. This questionnaire aims at undertaking a scientific approach to identify the perceived benefits of CM and determining the possible challenges faced by organizations that are considering this type of software solution.

As explained in Section 3.6.4, CM represents a business management responsibility, thus the main beneficiary of a CM solution is the business/control owner. Advocated by Gartner (2009), Hunt and Jackson (2010) and observed from the expert interviews, the Internal Audit and External Audit teams benefit as well from a CM implementation. As a result, the main beneficiaries are Business Owners, Internal Auditors and External Auditors. Professionals from these areas were targeted in the online questionnaire.

In order to attract the attention of as many respondents as possible, the sum of €1.00 for every complete response was promised to be donated to a charitable foundation. The first phase of reaching a large pool of respondents was by sending personalized e-mails to 160 professionals from the Internal Control, Internal Audit, External Audit, Business Process Management, Risk Management, Financial Control and SOX Compliance teams. The e-mail request is attached in APPENDIX A.

Additionally, the researcher joined a number of 36 LinkedIn[10] groups that were used as discussion forums by professionals within the above-mentioned target groups. The message contained in APPENDIX B was uploaded on the discussion page of every LinkedIn group from APPENDIX C. The questionnaire attracted also the attention of the Nederlandse

[10] http://www.linkedin.com/

Beroepsorganisatie van Accountants[11], a weekly electronic newsletter received by more than 20,000 Dutch accountants. The article is to be found in APPENDIX C. The questionnaire[12] was built on LimeService[13], a questionnaire service-platform to develop, activate and evaluate on-line questionnaires on a secure server. The lifetime of the questionnaire covered the period of two months, between the beginning of June and the end of July 2012.

The questionnaire was structured in three parts. The first part of the questionnaire asked for general information about the respondent, such as area of expertise, years of experience, department he/she is working in, etc. In order to measure the benefits of CM, three sets of statements for each target group (Business Owners: Table 8, Internal Auditor: Table 9, External Auditor: Table 10) were assembled based on literature review on CA and CM, and expert interviews. Respondents could agree or disagree to the collected statements to a certain degree, i.e. a four point Likert scale was used: Strongly Disagree, Disagree, Agree and Strongly Agree. The exclusion of the mid-point category was preferred in order to minimize the social bias that might appear from the participant desire to please the interviewer (Garland, 1991). The sets of statements are shown below:

Table 8: Statements for Business Owners

Nr.	Continuous Monitoring will:	Source
1.	Decrease the stress level of business owners during an audit.	Expert interviews
2.	Increase the quality of business decisions.	Nehmer (2003)
3.	Help business owners focus on the risk areas that are critical for reaching the established objectives.	Expert interviews
4.	Reduce the amount of time the staff needs for monitoring the controls.	Expert interviews
5.	Increase the likelihood of capturing at an early stage fraudulent and abusive actions.	Chan & Vasarhelyi (2011)
6.	Increase the operational performance of the business, i.e. by detecting, at an early stage, duplicate payments, misapplied warranties, incorrect discounts.	Vasarhelyi (2004); Hunt & Jackson (2010)
7.	Improve the awareness level by analyzing all the transactions on a real-time basis.	Expert interviews
8.	Increase the system security assurance level by detecting in real-time unauthorized access and manipulation of sensitive data.	Expert interviews
9.	Help in better identifying the opportunities for process improvements.	Chen (2003)
10.	Decrease the amount of financial loss through ongoing monitoring of purchases, payments, payroll, and travel & entertainment expenses.	Hunt & Jackson (2010)

[11] http://www.nba.nl/
[12] http://contmonitoring.limequery.org
[13] https://www.limeservice.com/

11.	Improve the internal control framework quality, i.e. reducing the number of controls by merging two controls into one.	Hunt & Jackson (2010)
12.	Increase the focus on measuring the quality of processes and data.	Expert interviews

Table 9: Statements for Internal Auditors

Nr.	Continuous Monitoring will:	Source
1.	Increase the reliability of financial statements through ongoing monitoring of financial transactions.	Vasarhelyi (2004); Zhao et al. (2004)
2.	Increase the transparency of the financial information provided to the shareholders.	Cangemi (2011)
3.	Provide a complete view of the effectiveness of all the transactions for which controls are set in place.	Rezaee et al. (2002); Vasarhelyi (2004); Chan & Vasarhelyi (2011)
4.	Increase the time spent on hard-to-test manual controls.	Expert interviews
5.	Decrease the amount of staff needed for audit.	Alles et al. (2006)
6.	Decrease the travel time needed for audits in multi-national organizations.	Expert interviews
7.	Decrease the costs for compliance.	Pathak et al. (2005); Hunt & Jackson (2010)
8.	Decrease the risk of non-compliance, which leads to penalties being issued by regulatory organizations.	Expert interviews
9.	Decrease the amount of stress of the internal audit team.	Expert interviews
10.	Level the amount of work throughout the whole year, rather than period-end close.	Nehmer (2003)
11.	Increase the reliability of the audit results.	Vasarhelyi (2004)
12.	Improve the quality of the internal audit by providing better audit evidence and scoping on the most important indicators, thus a more thorough audit trail.	Rezaee (2000); Rezaee et al. (2002); Alles et al. (2009)
13.	Ensure that the internal audit team will be better prepared for the external audit.	Chen (2003)
14.	Decrease the number of reporting follow-ups by reducing the amount of accounting errors that lead to manual follow-ups and time-consuming examinations.	Chen (20030)
15.	Reduce the time required for evaluating the effectiveness of controls due to higher accessibility to work papers and reports provided by the business.	Searcy & Woodroof (2003a)
16.	Provide the change from compliance-oriented audits to risk identification and process improvement-oriented audits.	Chan & Vasarhelyi (2011)

Table 10: Statements for External Auditors

Nr.	Continuous Monitoring will:	Source
1.	Increase the reliance on the work of the internal audit team.	Alles et al. (2009)
2.	Increase the efficiency of the review of the internal audit trail.	Chen (2003)
3.	Increase the quality of the audit.	Rezaee (2000)
4.	Increase the reliability of the audit.	Expert interviews
5.	Decrease the time required for testing the controls.	Expert interviews
6.	Decrease the audit fees that external auditors request to perform an audit.	Chen (2003); Gartner (2009)
7.	Decrease the travel time for external auditors.	Expert interviews
8.	Decrease the likelihood of future litigations.	Expert interviews
9.	Decrease the likelihood of rushing the audit to meet the examination deadlines.	Expert interviews
10.	Provide external audit firms the necessary capabilities to match the increase in complexity of future markets.	Expert interviews

The last part of the questionnaire contains an open-end question regarding the challenges towards CM as perceived by the respondents. The results of this question were compared to the challenges related to CA and the findings of the interviews on CM. A complete view of the questionnaire can be found in APPENDIX D.

4.2 Online Questionnaire Results

Due to the fact that the questionnaire was promoted on LinkedIn, the total number of participants that reached the questionnaire is unknown. However, personalized e-mails were sent to a sample of 160 participants. A total number of 143 completed and partially completed surveys were received, and a number of 85 completed responses were used to evaluate the proposed affirmations. Out of those 85 responses, no responses were discarded, outputting a response rate of 53,12%.

The following formula was used to calculate the response rate:

$$\mathrm{n} = \frac{\text{Nr of total complete responses}}{\text{Nr rezolved} - \text{Nr scoped\_out} + \text{Nr unrezolved}} = \frac{85}{143 - 0 + (160 - 143)} = 53{,}12\%$$

Overall, 85 respondents submitted their complete responses to the questionnaire. The reason why the number of respondents (

Table 11) per category exceeds the total is because participants were allowed to choose more than one area of expertise. In that case, statements which were linked to the expertise fields were presented to the respondent in the second part of the questionnaire.

Table 11: Online questionnaire number of respondents

Target group	Nr of respondents
Business Owners	42
Internal Auditors	46
External Auditors	16

The organizations the respondents work for span a number of various markets, i.e. Banking & Financial Services, Automobile, Aviation, Chemical Industry, Consumer Electronics, Defense, Health Care, Education, High Technology, Oil & Gas, Petrochemicals, Public Sector, Retail & Wholesale, Telecoms, Transport & Logistics.

The departments in which the participants exercise their professional skills are in agreement with the ones in scope of this research. These departments are: Accounting, Assurance, Audit, Enterprise Governance, Executive Board, Business Intelligence, Finance, External Reporting, External Compliance, General Management, Information Security, Risk Management, Internal Control.

Next, the results of the questionnaire are presented. For each group, the top five and last two statements (based on their mean values) will be analyzed. The complete over view of the results can be found in APPENDIX E.

Based on the expert interviews, the most important benefit of CM is the support that business owners (Table 12) are provided with in order to focus on the most critical risk areas, i.e. those that require urgent manual intervention, to meet their objectives. A CM solution would provide the means to measure the quality of enterprise data and the processes therein. The stress level of business owners is perceived to be decreasing when CM is used. These benefits have not been identified in the literature study. As already identified in the literature, the respondents predict an increase in the operational performance of the business. Fraud and abusive actions can be predicted as they happen if a CM solution would be in place.

Although the participants agreed with statements 8 and 11, these affirmations scored the lowest from the entire set. What is surprising is that improvements to the quality of the internal control framework (as advocated by Hunt & Jackson, 2010) scored the lowest.

Table 12: Business Owners questionnaire results

Nr.	Continuous Monitoring will:	Mean	Std. Dev.
3.	Help business owners focus on the risk areas that are critical for reaching the established objectives.	3,357	0,577
6.	Increase the operational performance of the business, i.e. by detecting, at an early stage, duplicate payments, misapplied warranties, incorrect discounts.	3,333	0,612
12.	Increase the focus on measuring the quality of processes and data.	3,333	0,57
5.	Increase the likelihood of capturing at an early stage fraudulent	3,286	0,673

	and abusive actions.		
1.	Decrease the stress level of business owners during an audit.	3,238	0,821
8.	Increase the system security assurance level by detecting in real-time unauthorized access and manipulation of sensitive data.	3,143	0,647
11.	Improve the internal control framework quality, i.e. reducing the number of controls by merging two controls into one.	3,095	0,759

The most important and the least important benefits for Internal Auditors are presented in Table 13. The top five benefits of CM are in agreement with the affirmations advocated by academicians in the CA field. These benefits include increased reliability of financial statements, better audit quality by the use of an audit trail, increased focus on process-improvements audits, the examination of the entire population of transactions and increased reliability of the audit results.

The statements that receive the lowest agreement scores are the decreased amount of staff, as advocated by Alles et al. (2006), and the decreased amount of stress, as mentioned in the expert interviews.

Table 13: Internal Auditors questionnaire results

Nr.	**Continuous Monitoring will:**	**Mean**	**Std. Dev.**
1.	Increase the reliability of financial statements through ongoing monitoring of financial transactions.	3,413	0,617
12.	Improve the quality of the internal audit by providing better audit evidence and scoping on the most important indicators, thus a more thorough audit trail.	3,261	0,648
16.	Provide the change from compliance-oriented audits to risk identification and process improvement-oriented audits.	3,174	0,769
3.	Provide a complete view of the effectiveness of all the transactions for which controls are set in place.	3,109	0,795
11.	Increase the reliability of the audit results.	3,087	0,661
5.	Decrease the amount of staff needed for audit.	2,739	0,681
9.	Decrease the amount of stress of the internal audit team.	2,283	0,584

Table 14 contains the external auditors' responses to the questionnaire. The benefits that have the highest scores, i.e. increased quality of the audit, efficiency of the review of the audit trail and increased reliance on the internal audit's work, are in line with the academicians' findings. The increase in the reliability of the audit represents a new finding. The decrease in travel time and likelihood of future litigations have received the lowest scores.

Table 14: External Auditors questionnaire results

Nr.	Continuous Monitoring will:	Mean	Std. Dev.
3.	Increase the quality of the audit.	3,375	0,5
2.	Increase the efficiency of the review of the internal audit trail.	3,313	0,602
4.	Increase the reliability of the audit.	3,313	0,479
1.	Increase the reliance on the work of the internal audit team.	3,25	0,577
10.	Provide external audit firms the necessary capabilities to match the increase in complexity of future markets.	3,063	0,574
7.	Decrease the travel time for external auditors.	2,625	0,719
8.	Decrease the likelihood of future litigations.	2,563	0,512

The challenges for CA and CM identified in Section 3.5 and 3.6 respectively were compared to the ones provided by the respondents. This step is necessary to determine whether the CM would face the same challenges as CA and whether the interviewees' answers are unique.

The complete list of challenges is to be found in APPENDIX E. Several perceived impediments toward CM adoption that were not mentioned by the means of literature study or interview findings are presented next. One challenge stated by the Business Owners is the identification of the right set of controls for monitoring. The current research attempts to determine and relate the relevant dimensions for prioritizing internal controls, thus overcoming this challenge. Cooperation between business and assurance functions is also one impediment toward CM adoption. The relationship between this challenge and the IT artifact is mentioned in the following chapter. Another challenge is represented by the cultural change in terms of the way alerts are communicated and handled.

One challenge, as observed by the Internal Auditor group and not mentioned in the literature, would be the mind shift in internal control which requires a thorough insight in the data models and processes. From the External Audit group's challenges are worth mentioning the need to automate processes and the need to ensure that the controls used for CM are relevant from an operational and financial point of view, otherwise the business will not pay attention to it. Another challenge would be the way false positives are interpreted over time by the business. One respondent stated that the biggest impact of CM would be in the work of the quality team and in the management of exceptions. This is a substantial change as it impacts the risk organization structure and the external audit approach.

Chapter 5 Internal Control Prioritization Tool

In order to answer RSQ4 and identify the relevant dimensions of internal control prioritization, this chapter will describe the development of the Internal Control Prioritization Tool (ICPT). The initial version of the ICPT was assembled based on the analysis of two Internal Control Matrices (ICM) provided by the organizations that were involved in this research and on observations during the implementation phase of CM at one of the companies. The evaluation step in the Design Science Research method states that the artifact has to be evaluated in order to assure that it solves the issue at hand. Consequently, three expert interviews were carried out with the intent to improve the quality of the initial version of the tool. RSQ5 was answered by performing two case studies. The ICPT was applied on their ICM and the results were discussed during a follow-up interview and a comparison with the controls implemented with a CM solution at one of the organizations. Moreover, an application process was assembled to explain how the ICPT must be used.

The final version of the tool is described in Section 5.1 and all the outcome of the evaluation phase is described in Section 5.2. Section 5.3 contains the application process of the ICPT. The application of the ICPT and its output are discussed in Section 5.4.

5.1. ICPT Overview

In order to present a clear view of what the purpose of the ICPT is, a fragment of an ICM is presented in Figure 12. The scope of the ICPT is to prioritize the three controls based on a number of 8 dimensions, as shown in Figure 14. After the ICPT is applied on the ICM, i.e. a parameter was assigned to every dimension for every control, and the values are added, then a prioritization list is outputted (see Figure 13).

Process	SubProcess	Risk	Control	Control Objective	Control Description
General Ledger	G/L Maintenance Activity	Changes to the chart of accounts are approved.	Postings are made to invalid accounts which could lead to misstatement in the financial reporting.	GL account additions and changes are approved.	All GL account additions and changes are approved by an authorized individual.
Purchase and Payables	Ordering	Long outstanding open purchase orders are investigated and resolved.	There is a risk of financial loss if short deliveries, damaged goods received or incorrect goods received are not followed up promptly.	Purchase manager periodically reviews open purchase order/purchase requisition reports for timely resolution of aged items.	Purchase manager periodically reviews open purchase order/purchase requisition > 20K reports for timely resolution of aged items using program RTS150. All open items older that one month are investigated and open items that cannot be resolved are commented. The reports are signed off and archived as evidence or review.
General Ledger	Posting of Sub ledger to the General Ledger	Postings from subledgers are not completely and accurately recored in G/L.	The system is monitored to ensure postings have been processed successfully.	Suspense, invalid or other rejected or improper automated postings are analyzed and resolved on a timely basis.	The program RT650 is monitored to ensure postings have been processed successfully. Errors in RT650 are resolved and monitored using RT100 on a regular basis.

Figure 12: Fragment of Internal Control Matrix

Process	SubProcess	Control	D1	D2	D3	D4	D5	D6	D7	D8	Total
General Ledger	Posting of Sub ledger to the General Ledger	The system is monitored to ensure postings have been processed successfully.	semi-automated	detective	daily/weekly	high	high	Yes	Yes	No	**10**
General Ledger	G/L Maintenance Activity	Postings are made to invalid accounts which could lead to misstatement in the financial reporting.	semi-automated	preventive	annually	medium	medium	No	Yes	Yes	**7**
Purchase and Payables	Ordering	There is a risk of financial loss if short deliveries, damaged goods received or incorrect goods received are not followed up promptly.	semi-automated	detective	monthly/quaterly	low	high	Yes	No	No	**6**

Figure 13: ICPT applied

The 8 dimensions of the tool, their parameters and their respective values are detailed below.

The first dimension refers to the automation level of a control. Described in Section 3.3, controls can be manual, semi-automated or automated in nature. A manual control requires laborious human work, therefore it is scoped out of a CM solution and it receives a value of 0. An automated control represents an Application Configuration control, an Authorization control or a Segregation of Duties control. The last two types of controls are the core of assuring proper functioning of processes within an enterprise or financial system. Failure of any of the two would result into abusive actions in the system and critical risks. For this reason, Authorization and SOD controls should be properly dealt with before implementing CM. In terms of Application Configuration controls, their selection for CM would result in only an increased level of the quality of testing, whereas the selection of a semi-automated control leads to improved quality testing but also a decreased amount of manual work performed by the user. Consequently, an automated control receives a value of 1, and a semi-automated control a 2.

The second dimension concerns the type of a control. In Section 3.3.3 Moeller (2005) states that preventive controls are essential in an internal control system as they are the first line of defense. They determine the quality of the enterprise system. Preventive controls score higher than detective control because the later are designed to detect errors and deviations from normal behavior after they have occurred.

Dimension three deals with how often a control is being tested. A control that is tested on a daily/weekly basis suggests that it cover critical transactions within business processes, receiving higher values than controls that are inspected on longer periods of time, such as monthly/quarterly or even annually.

The fourth dimension refers to the level of impact on key General Ledger[14] accounts. Given the fact that the income statements and balance sheets are extracted from the General Ledger (Mills, Call & Drew, 2000), a control that investigates transactions that pose a high level of impact receives the value 2, while a medium and a low level receive a score of 1 and 0,

[14] General Ledger represents the most important accounting record of an organization.

respectively. Depending on the amount and value of transactions of any given organization, a further classification of what precisely high, medium and low mean is impossible to be set.

Dimension five measures the ERP system knowledge of the data a control examines. If anyone in the organization, i.e. business/financial controller, auditor or IT staff, has extensive knowledge of the underlying system set-up such as tables and fields, then it is categorized as high and receives the value 2. Knowing only the system program/report outputs a medium level of knowledge, while no knowledge at all received the value 0.

Dimension six measures the demand for root cause capabilities. If the control tests a data set that requires drill-down capabilities up to a granular level, then the control owners is required to increase his/her effort on examining that data than a control that does not demand this capability. For this reason, a former is more important than the later, and it receives a 1.

The seventh dimension measures whether manual changes can be performed within the business workflow the control is testing. One such example would be manual reconciliations between various financial accounts. Another example is represented by manually adjusting the data between the approval of a purchase order and the release of the payment. Controls that test transactions in which manual interventions can be performed are regarded as more important than the ones for which no manual adjustments are allowed.

Dimension eight evaluates the activities investigated by controls related to the impact on the quality of master data records. What is the point of having the system check for a tolerance limit when a user approves a payment if that tolerance is limitless? Other examples refer to the changes to the limit amount of a payment, changes of bank accounts of existing vendors, adding fictitious vendors into the system, etc. The quality of Master Data is a precondition for a good functioning system and non-interrupted business processes therein. A control that examines the quality of master data is ranked with a 1, whereas a control that does not perform that type of inquiry receives a 0.

Dimension No.	Dimension	Parameters	Values
D1	Automation level	Automated Semi-automated Manual	Automated = 1 Semi-automated = 2 Manual = 0
D2	Control type	Preventive Detective	Preventive = 1 Detective = 0
D3	Frequency	Daily/weekly Monthly/quartely Annually	Daily/weekly = 2 Monthly/quaterly = 1 Annually = 0
D4	Level of impact on key G/L accounts	High Medium Low	High = 2 Medium = 1 Low = 0
D5	ERP system knowledge	High Medium Low	High = 2 Medium = 1 Low = 0
D6	Root cause analysis	Yes No	Yes = 1 No = 0
D7	Manual intervention/adjustments of data	Yes No	Yes = 1 No = 0
D8	Impact on quality of Master Data (customer, item, pricing, supplier)	Yes No	Yes = 1 No = 0

Figure 14: Internal Control Prioritization Tool

5.2. ICPT Evaluation

Critical to this research is the evaluation of the artifact. Without this step, design science research is incomplete. Three interviews were conducted with experts (Table 15) in the fields of accounting, IT and CM in order to evaluate the prioritization tool and check for possible improvements. In order to acquire pertinent observations, the respondents were selected based on their extensive knowledge in the above-mentioned areas. The outcome of their comments yielded changes that were processed in order to improve the quality of the tool.

Table 15: Interview respondent overview

Respondent type	Sector	Category	Size FTE
Product Owner	Technology	Computer Software	100-200
Accounting & Internal Control Professor	Education	Research	-
External IT Auditor	Consultancy	Audit	100,000+

The initial prioritization tool was composed of 19 dimensions. The initial ICPT together with a list of questions (Table 16) were submitted to the experts prior to the interviews. The quality measures were used from the internal quality criteria mentioned by Brinkkemper, Saeki

and Harmsen (1999). This step allowed the interviewees to prepare in advance and create an in-depth opinion about the artifact.

Table 16: Quality measure questions

Quality measure	Questions
Completeness	Is the tool complete? Are there any improvements to be made?
Consistency	Is the tool consistent? Is it correct and meaningful?
Efficiency	Is the tool efficient?
Applicability	Can the tool be applied in practice?
Reliability	Is the tool reliable? Can it be applied in any type of company, regardless of the industry it operates?

The complete modifications to the tool are depicted in Table 17. These changes reduced the number of dimensions from initially 19 to 8.

Table 17: Changes applied to the ICPT

Dimension	Change
Impact on key G/L accounts? (Yes – No)	One interviewee stated that most of the internal controls influence in one way or another key G/L accounts, thus it makes more sense to evaluate the control's level of impact on key G/L accounts and have as parameters Low, Medium and High. This dimension was renamed to: **Level of Impact on key G/L accounts.**
Volume&Value – Materiality (Low-Medium-High)	The 'Level of Impact on key G/L accounts' dimension already refers to the materiality of the transactions. For this reason, this dimension was removed from the tool.
Knowledge of system reports	The 'ERP system knowledge' dimension inquires whether the underlying system set-up, i.e. tables, fields, is known. As a result, 'Knowledge of system reports' is not relevant anymore, and it was removed.
SOX – External Reporting	The interviewees argued that public companies would be the first ones to consider CM solutions, thus this dimension would not add any value to the tool. Consequently, it was removed from the tool.
Duplicate control	One step of the ICPT Application Process is to remove irrelevant controls before the application of the tool. Consequently, this dimension is removed from the tool.
Field Audit Trail	This dimension refers to the history backlog of a control. One interviewee mentioned that 'Level of Impact on key G/L accounts' and 'Impact on quality of Master Data' dimensions already cover this one. Consequently, this dimension were removed from the tool.
SOD control	One of the interviewees mentioned that failure of any SOD

	controls would result into abusive actions in the system and critical risks. For this reason, SOD controls should be properly dealt with before implementing CM. Consequently, SOD controls should have priority over any other type of control. Consequently, this dimension is scoped out of the application of the tool.
Authorization control	One of the interviewees also mentioned that failure of any Authorization controls would result into abusive actions in the system and critical risks. For this reason, Authorization controls should be properly dealt with before implementing CM. Consequently, Authorization controls should have priority over any other type of control. Consequently, this dimension is scoped out of the application of the tool.
Control tested by Business Owners?	These dimensions refer to the professionals that must assess the efficiency of a specific control. Due to the fact that all three stakeholders were identified as beneficiaries from a CM solution, these dimensions were removed from the tool.
Control tested by Internal Audit?	
Control tested by External Audit?	
Drilldown capabilities	One interviewee suggested that the dimension should be renamed to '**Root cause analysis**'.
Change frequency of control	The interviewees argue that the majority of controls do not change that often, once they are set-up. As a result, this dimension was removed.
Changes to Master Data	One interviewee suggested that the dimension should not refer to whether there are changes on the master data, but whether there is an impact on the quality. He stated "*what difference does it make if the credit limit field is active but the limits for users are set to €10 mil, or the other way around?*". Consequently, the dimension was renamed to '**Impact on quality of Master Data**'.

Overall, the interviewees agreed that the tool "*the tool is valid, i.e. it focuses on the right dimensions to prioritize controls, but the reliability cannot be specified at this point because it has never been tested".* One interviewee mentioned that "*the only thing that is missing is the importance of the process, but you don't get to change the tool, but only the way you apply it*". It was also stated that "*the tool is complete and that it is a useful thing"*. Another participant expressed that "*for the high level prioritizing I think the tool is consistent*". In terms of applicability, it was stated that it should be possible to be applied in practice, but the output of the prioritization list should differ per company.

5.3. ICPT Application Process

In order to understand how the ICPT is applied in practice, the application process is presented in Figure 15.

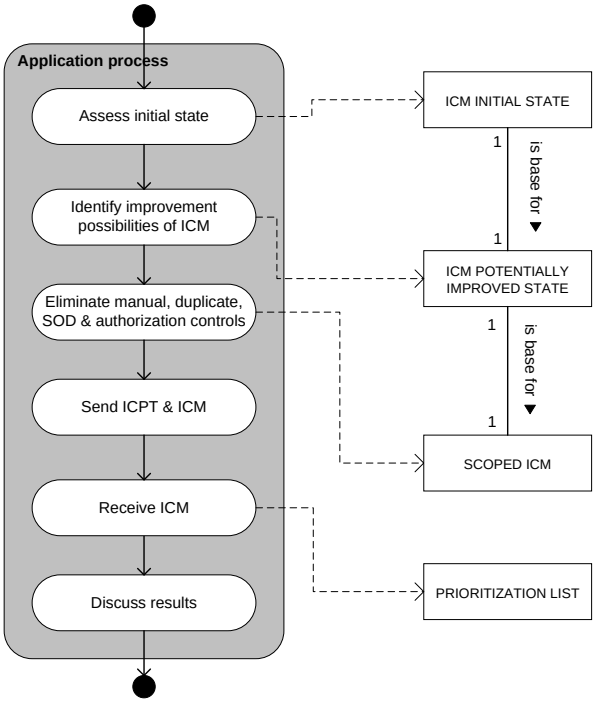

Figure 15: ICPT application process

The assessment of the initial state of the ICM is the first step in the Application process of the ICPT. This step gives us an overview of the ICM, such as number of processes, sub-processes, risks, controls, control objectives, their description, the automation level and their types.

The next step consists of identifying possible improvements of the ICM. The reason for including this phase is that Hunt and Jackson (2010) advocate that CM improves the control framework by automating manual controls and this research provides the means to test that affirmation.

Next, the manual, duplicate, SOD and Authorization controls are removed from the ICM. This step is essential in the correct application of the tool. As mentioned in Section 5.2, SOD and Authorization controls are crucial for any enterprise system, thus they should be considered first in a CM project. The exclusion of the duplicate controls form the ICM, if any, would reduce the time required for applying the tool. The manual controls are scoped out because their level of automation. This ICM would contain the controls that would be in scope of a CM project.

Next, the potentially improved ICM and the ICPT are sent to the organization for filling in all the parameters for each control in the matrix. One example can be observed in Figure 16.

Process	SubProcess	Control	D1	D2	D3	D4	D5	D6	D7	D8
General Ledger	Posting of Sub ledger to the General Ledger	The system is monitored to ensure postings have been processed successfully.								
General Ledger	G/L Maintenance Activity	Postings are made to invalid accounts which could lead to misstatement in the financial reporting.								
Purchase and Payables	Ordering	There is a risk of financial loss if short deliveries, damaged goods received or incorrect goods received are not followed up promptly.								

Figure 16: ICM and ICPT

In the following two steps, the ICM is received, the total score per control is calculated and the prioritization list (Figure 17) is discussed with the organization in order to evaluate the results.

Process	SubProcess	Control	D1	D2	D3	D4	D5	D6	D7	D8	Total
General Ledger	Posting of Sub ledger to the General Ledger	The system is monitored to ensure postings have been processed successfully.	semi-automated	detective	daily/weekly	high	high	Yes	Yes	No	**10**
General Ledger	G/L Maintenance Activity	Postings are made to invalid accounts which could lead to misstatement in the financial reporting.	semi-automated	preventive	annually	medium	medium	No	Yes	Yes	**7**
Purchase and Payables	Ordering	There is a risk of financial loss if short deliveries, damaged goods received or incorrect goods received are not followed up promptly.	semi-automated	detective	monthly/quaterly	low	high	Yes	No	No	**6**

Figure 17: Prioritization List

5.4. Case Studies

Yin (1984) describes the case study research method as "*as an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used*". The case study approach was selected for this research study as it addresses answering "how" questions and the behavior of the parties involved in the study cannot be manipulated. Darke, Shanks and Broadbent (1998) argue that case studies are ideal for testing of theory. Multiple case studies are examined to apprehend the differences and similarities between the various cases and provide sufficient reliability and robustness to the research (Yin, 2003). In this research, the final version of the IT artifact, the ICPT, was used to prioritize the controls of two organizations. The evaluation of the output acted as a measure to ensure the validity of the artifact.

Planning is a crucial element for the success of a multiple case study. Yin (1984) suggests following four phases in order to assure that, namely (1) designing the case studies; (2) conducting the case studies; (3) analyzing the case studies evidence; and (4) formulating the conclusions and possible recommendations. Darke et al. (1998) point out that various data collection techniques should be combined when performing case studies. Interviews, observations, questionnaires and document analysis represent a few examples of such data collection techniques. In the current research both interviews and document analysis were carried out. In addition, the interviews were electronically recorded in order to focus on the topic at hand.

5.3.1. Case Studies Overview

The two organizations are listed on well-known stock exchanges around the globe, they operate in the private sector and they are technology-oriented (Table 18). Due to the significant level of sensitivity of company data, the names of the multinationals are kept anonymous. For this research stage, an ICM from each party involved was collected and interviews (Table 19) were performed at the end with experts from the Compliance/Finance areas with the intent to evaluate the results of the application of the tool.

Table 18: Case studies overview

Name	Sector	Branch	Size FTE
ORG1	Technology	Manufacturing	30,000+
ORG2	Technology	Medical equipment & Supplies Manufacturing	1,000 – 5,000

Table 19: Interviews respondent overview

Respondent type	Sector	Category	Size FTE
Compliance Leader	Technology	Manufacturing	30,000+
Head of Financial Control	Technology	Medical equipment & Supplies Manufacturing	1,000 – 5,000

The first step of the ICPT Application Process consists of analyzing the initial state of the ICM and providing an overview of the collected data. The processes and controls per company were analyzed and categorized, as can be observed in Table 20 and Table 21.

Table 20: ORG1 Controls per process overview

Process	Nr of Controls
Purchase-to-Pay	58
Production & Inventory management	45
Order-To-Cash	40
Finance-Accounting & Controllership	35

Fixed Assets	23
HR	26
IT	13
Total	**240**

Table 21: ORG2 Controls per process overview

Process	**Nr of Controls**
General Ledger	32
Inventory and Manufacturing	31
Purchase and Payables	85
Revenue and Receivables	65
Revenue and receivables - rental	32
Revenue and receivables - service	41
Total	**286**

Step 2 and Step 3 of the ICPT Application Process were performed. The analysis of the ICM was carried out together with an expert in the field of auditing financial controls and CM implementations (Table 22).

Table 22: Interview respondent overview

Respondent type	**Sector**	**Category**	**Size FTE**
Product Owner	Technology	Computer Software	100-200

Controls that contained the same description and name were tagged as duplicate. Automated and semi-automated controls that were tagged as SOD and Authorization controls were scoped out. Next, based on the professional experience of the expert, an analysis was performed on the manual controls in order to determine whether their degree of automation can be increased. The transformation of a control was based on whether the control is being executed in the system, or using the system, or if, to the expert's knowledge, the ERP system that the organization has in use can support this manual control or make it easier. This procedure follows the actions undertaken during the application of the ICPT. Table 23 and Table 24 contain the controls in scope for the application of the ICPT.

Table 23: ORG1 Application Process overview

Control Type	**Initial state**	**% Total**	**Potential improvement manual controls**	**Scoped out controls**	**In scope for CM**
Automated	21	9%	7	24	4
Semi-automated	54	23%	75	27	102
Manual	165	68%	83	83	0
Total	**240**	**100%**	**165**	**134**	**106**

Table 24: ORG2 Application Process overview

Control Type	Initial state	% Total	Potential improvement manual controls	Scoped out controls	In scope for CM
Authorizations	95	33%	0	95	0
Automated	38	13%	2	10	30
Default system behaviour	34	12%	0	34	0
Manual	32	11%	9	9	0
Semi-Automated	87	30%	21	15	93
Total	**286**	**100%**	**32**	**163**	**123**

The next step of the ICPT Application Process consisted of the submission of the ICM that contained the controls in scope of the prioritization and the ICPT. The detailed overview of the ICPT that was sent to ORG1 and ORG2 can be found in APPENDIX E. Next, the ICMs containing the parameters for all the dimensions were received by the researcher and based on the values given for each parameter in the ICPT, the scores for each control were calculated.

5.3.2. Case Studies Analysis

ORG1

In the case of the first organization, the top 80 controls of the highest-to-lowest prioritized list were selected, grouped by process and compared to the controls that were in scope for CM. The results are depicted in Table 25. One interesting finding is that the controls mapped to financial processes have the highest selection percentage.

Table 25: ORG1 Top 80 ranked controls

Process	In scope for CM	Top 80 prioritized controls	%
Purchase-to-Pay	20	20	100%
Production & Inventory management	24	17	71%
Order-To-Cash	18	13	72%
Finance-Accounting & Controllership	13	11	85%
Fixed Assets	14	9	64%
HR	15	9	60%
IT	2	1	50%
Total	**106**	**80**	**75%**

These results were discussed with the organization during a follow-up interview. The interviewee agreed that "*the controls from this prioritization list can be used as a starting*

point when implementing a CM solution". After a closer look at the list, the participant identified that some controls within the Fixed Assets process have scored more than he expected and did not believe that all 9 controls should receive such a high importance. He stated that "*this list can be used to build the CM solution gradually by focusing in the beginning on a few processes or a limited number of controls or on a combination thereof*". As a consequence, further improvements can be made to scope out controls that are not that important for the initial phase of a CM. This can be accomplished by "*combining two controls that belong to the same risk and have the same value or choosing only one for implementation*".

Furthermore, the participant suggested that processes should also receive a value and have the total score of the control multiplied by the value of its process. He mentioned that this would improve the tool's reliability. "*The Payroll process is key in an audit firm, whereas Assets Management is not that critical"*. In this way, controls would be selected depending on the core business of the organization. It might also be the case that some processes are not desired to be included in the CM at all. Overall, based on its output, the ICPT received positive feedback as it is a "*useful and easy-to-use tool*".

ORG2

In the case of the second organization, the output of the application process was compared with the controls that were implemented in the CM solution. In this way, a 1-1 mapping was performed and a matching percentage was obtained. The total number of controls implemented with CM was 80. In order to be able to compare the CM implemented controls with the prioritized ones, the top 80 controls with the highest scores were selected from the prioritization list. The controls were grouped by process and then matched with each other. The final result can be observed in Table 26u. An overall matching percentage of 69% was obtained, having the lowest and highest matching status of 29% and 86% respectively. The trend that was observed in the first case study can be seen here as well. The controls mapped to financial processes have the highest matching percentage.

Table 26: ORG2 Matching controls – 1st comparison

Process	**CM implemented controls**	**Prioritized controls**	**Matching**	**Matching %**
General Ledger	17	14	12	86%
Inventory and Manufacturing	5	7	2	29%
Purchase and Payables	23	20	14	70%
Revenue and Receivables	26	25	21	84%
Revenue and receivables - rental	5	7	3	43%
Revenue and receivables - service	4	7	3	43%
Total	**80**	**80**	**55**	**69%**

Based on the suggestions from the follow-up interview with ORG1, the controls were selected depending on each process and not the entire list. To exemplify, the CM

implementation covered 17 controls from the General Ledger area. The same amount of controls was chosen from the prioritization list of the General Ledger controls. The same technique was applied for all the other process areas. An overall matching percentage of 74% was obtained, having the lowest and highest matching status of 20% and 88% respectively. Table 27 contains the results. An interesting finding is that the application of the ICPT yields higher results when the controls are divided by process.

Table 27: ORG2 Matching controls – 2nd comparison

Process	CM controls	Prioritized controls	Matching	Matching %
General Ledger	17	17	15	88%
Inventory and Manufacturing	5	5	1	20%
Purchase and Payables	23	23	16	70%
Revenue and Receivables	26	26	21	81%
Revenue and receivables - rental	5	5	3	60%
Revenue and receivables - service	4	4	3	75%
Total	**80**	**80**	**59**	**74%**

One of the most significant discoveries that were observed during the case studies is the cooperation between business and assurance functions while applying the ICPT. The ICPT provides a firsts step in narrowing this gap. Furthermore, no improvements were noticed during the CM implementation as suggested by Hunt and Jackson (2010). We have noticed, however, that if the ICPT is applied, 49% of the manual controls for ORG1 and 71% for ORG2 can be partially automated.

Finally, ORG1 stated that CM should be used as a pilot in certain geographical areas or countries, and then expand. The same was observed with ORG2, as CM was implemented in one division, and based on its future success rate, it will be expanded to others as well..

Chapter 6 Discussion

This chapter describes the limitations identified in this research as well as the threats to its validity and the steps that were undertaken to minimize these threats. Certain limitations are identified, such as limited number of case studies, the fact that the research was carried out by one researcher and only one CM implementation was observed during the period of this research. Furthermore, validity is divided into four parts: construct, internal and external validity, and reliability. Various actions were performed for each type throughout the duration of this project.

Section 6.1 contains the research limitation, while Section 6.2 discusses the risks that might damage the validity of the research and the actions that were undertaken to minimize those risks.

6.1. Research Limitations

Even though multiple steps were executed to ascertain the validity of this research, the project is still subject to several limitations. The main limitation is represented by the limited number of case studies. In multiple case studies several cases are examined to apprehend the differences and similarities between the various cases and provide sufficient reliability and robustness to the research (Yin, 2003). Despite having two organizations involved into this research, the differences between their processes do not provide sufficient assurance for generalization.

The period in which the online questionnaire was active represents a limitation. The period covered the months of July and August when many professionals are on holiday. Also, the rather low number of external auditors that answered the questionnaire compared to the rest of the target groups is a limitation of the results for that group.

Another limitation is identified by the fact that only one organization (ORG2) implemented a CM solution, making it impossible to map the prioritized controls of ORG1 to a list of implemented ones. Consequently, the application of the ICPT to ORG1 only provided a base for qualitative analysis.

Two internal control matrixes in the case studies section were analyzed for further improvements. One limitation that might arise from this procedure is that the automation potential was based on the opinion of only one expert, and no cost/benefit analysis was performed by the organization to actually determine whether those improvements are beneficial.

Lastly, Runeson and Hoest (2008) state that it is desirable to analyze the data in a research attempt by two or more researchers in a separate manner so that the same final conclusions are reached. This gap was covered by the multiple expert evaluations of the tool.

6.2. Validity

Messick (1989) defines validity as an evaluative reasoning regarding the level to which the research question identified in Section 1.2 is answered by this research. The validity of this research was assured by pursuing the scientific research techniques that were explained in Chapter 2. Moreover, bias was avoided by performing all the validity steps advocated by Yin (2003):

- **Construct validity** – The development of ICPT was based on analyzing the documentation from the organizations involved in the case studies, and the evaluation of the tool and its further refinement was conducted by means of expert interviews.
- **Internal validity** – It is threatened by the analysis of the results by only one researcher. This issue was overcome by performing a follow-up interview with ORG1, and a one-to-one control mapping between the controls implemented in a CM implementation and the ones from the prioritization list.
- **External validity** – It is threatened by the limited number of case studies and by the different processes they have set in place. Also, the different markets the firms operate in threaten the validity of the IT artifact. Nonetheless, these issues were overcome by the expert interviews and their positive responses on the quality measures of ICPT, and the positive outcome of the application of the tool in the case studies.
- **Reliability** – Due to the fact that the research procedures aimed at describing the case studies as clearly as possible, the researcher expects that this research is repeatable, and another researcher that would follow the same steps will conclude similar results.

Chapter 7 Conclusions

The main research question of this project is "*How can organizations be assisted in prioritizing their internal controls for Continuous Monitoring?*". This question is answered by examining the results of the research approaches that were detailed in the previous chapters. Opportunities for future research are outlined in the last section of this chapter.

7.1. Research Questions

The above-stated research question was split into three parts that were answered in various phases of this research. The first sub-question was addressed through literature review and expert interview. The second and third sub-questions were answered by the means of literature study, expert interviews and an online questionnaire. The fourth sub-question was the result of case study documentation and the artifact was evaluated and refined through expert interviews. Finally, the answer of the fifth sub-question was given by using two case studies and performing follow-up interviews.

RSQ1: What does Continuous Monitoring represent and what are the stakeholders that benefit the most from a Continuous Monitoring implementation?

CM represents a data analysis software solution with the ability to ensure that the internal controls function as intended and business transactions operate properly. CM is primarily intended for business owners by delivering valuable data on a continuous basis from the enterprise system and detecting opportunities for business processes improvements and diminishing financial losses.

CM supports trending over time, and alerts that contain outliers, based on predetermined limits and thresholds, are sent to the controllers based on the examination of the entire population of transactions. Every notification, review and follow-up steps are recorded within the system, supplying the necessary evidence for an audit trail. As such, it also represents a tool that helps the work of the internal and external audit team as documentation exists whether internal policies are followed in an appropriate manner and exceptions are documented properly. Consequently, the beneficiaries of a CM software solution are the Business Owners, Internal Audit team and the External Audit team.

RSQ2: What are the most valuable gains from implementing a Continuous Monitoring software solution as distinguished by the identified stakeholders?

Although some of the gains that were perceived as valuable by the respondents were identified in the area of Continuous Auditing, this research reveals a number of benefits that resulted from the interviews and received a high level of agreement.

From a business owner perspective, the support that CM provides with in order to focus on the most critical risk areas, i.e. those that require urgent manual intervention, to meet their

objectives, was seen as the most important. Another finding is that a CM solution would provide the means to measure the quality of enterprise data and the processes therein. The statement that the stress level of business owners is perceived to be decreasing when CM is used was considered important. Surprisingly, the statement that CM improves the quality of the internal control framework (as advocated by Hunt & Jackson, 2010) scored the lowest.

The most important benefits for Internal Auditors are in agreement with the affirmations advocated by academicians in the CA field. These benefits include increased reliability of financial statements, better audit quality by the use of an audit trail, increased focus on process-improvements audits, the examination of the entire population of transactions and increased reliability of the audit results. The statements that receive the lowest agreement scores, however, are the decreased amount of staff, as advocated by Alles et al. (2006), and the decreased amount of stress, as mentioned in the expert interviews.

From an external auditor's point of view, the benefits that have the highest scores, i.e. increased quality of the audit, efficiency of the review of the audit trail and increased reliance on the internal audit's work, are in line with the academicians' findings. The increase in the reliability of the audit represents a new finding. The decrease in travel time and likelihood of future litigations, as identified from the interviews, have received the lowest scores.

RSQ3: What are the challenges that organizations need to overcome when considering an implementation of Continuous Monitoring software tools?

Several challenges toward CM adoption that were not mentioned by the means of literature study or interview findings were identified in this research. One challenge stated by the business owners is the identification of the right set of controls for monitoring. This statement adds extra value to the artifact assembled in this project. Cooperation between business and assurance functions is also one impediment toward CM adoption. Another challenge is represented by the cultural change in terms of the way alerts are communicated and handled.

One challenge, as observed by internal auditors and not mentioned in the literature, would be the mind shift in internal control which requires a thorough insight in the data models and processes.

External auditors mentioned as challenges the need to automate processes. It was also stated that there is a need to ensure that the controls used for CM are relevant from an operational and financial point of view, otherwise the business will not pay attention to it. Another challenge would be the way false positives are interpreted over time by the business. One respondent stated that the biggest impact of CM would be in the work of the quality team and in the management of exceptions. This is a substantial change as it impacts the risk organization structure and the external audit approach

RSQ4: What are the relevant dimensions in internal control prioritization and how can they be related to each other?

The Internal Control Prioritization Tool contains 8 dimensions, each with specific parameters and values:

- Automation level: automated, semi-automated, manual (1, 2, 0);
- Control type: preventive, detective (1, 0);
- Frequency: daily/weekly, monthly/quarterly, annually (2, 1, 0);
- Level of impact on key G/L accounts: high, medium, low (2, 1, 0);
- ERP system knowledge: high, medium, low (2, 1, 0);
- Root cause analysis: yes/no (1, 0);
- Manual intervention/adjustments of data: yes/no (1, 0);
- Impact on quality of Master Data: yes/no (1, 0).

For every control the above dimensions must be answered with a parameter. Summing all the values for each dimension will output an overall score for every control.

RSQ5: How can the Internal Control Prioritization Tool be applied in practice?

In order for the ICPT to be applied in practice, an ICPT Application Process was presented for guidance. As a first step, the initial state of an ICM is determined. The second step tried to identify possible improvements to the automation level of the manual controls. Step 3 eliminates the irrelevant controls, i.e. manual and duplicates, but also critical controls that should already be included in a CM project. Next the ICPT is applied on the scoped ICM, and the results are analyzed.

In this research, two case studies were conducted at two publicly listed organizations, ORG1 and ORG2. ORG1 was considering implementing a CM solution, whereas ORG2 has implemented CM during the period of this study. The output of the first application of the ICPT resulted in a qualitative analysis, while the second application resulted in a quantitative analysis. The output of the first case study led to positive feedback from ORG1, agreeing that the prioritization list can be used as a starting point when choosing which controls to focus on in a CM project.

The analysis of the second case study outputted more concrete results. The mapping of the top 80 controls that were implemented in CM with the top 80 controls of the prioritized list showed a matching percentage of 69%. Splitting the controls by processes and selecting the same amount of controls from the prioritization list and the practical implementation, yielded a higher matching score of 74%. These results show that the tool is reliable and valuable. It was also observed that the controls with the highest scores in the prioritization list belong to financial areas.

It was also observed that CM tends to be started in one area of the organization and based on its successful and adoption rate, it will be expanded.

RSQ: How can organizations be assisted in prioritizing their internal controls for Continuous Monitoring?

In conclusion, the answer to the main research question is given by the assembly of the Internal Control Prioritization Tool, in which the relevant dimensions were identified. Furthermore, an application process was detailed in order to provide guidance on how to apply the tool.

7.2. Future Research

Based on the limitations and validity threats presented in Chapter 6, several areas for future research can be observed.

Firstly, future research can look into the changes that Continuous Monitoring brings to organizations. It is interesting to discover whether the identified gains improve the operational effectiveness and provide increased business assurance in the long run, or if CM is just an additional tool whose capabilities will not be fully exploited.

In this research the controls were mapped to processes, but sub-processes were disregarded. It would be interesting to research the type of influence sub-processes have on the prioritization tool and the prioritization list.

Lastly, the ICPT was applied to only two organizations. For this reason, the possibility of generalizations is limited. Additional research should be conducted to apply this prioritization tool to more companies, and analyze the outcome. It is also very important to perform the analysis at companies that are implementing a CM solution, in order to have concrete results.

Lastly, an interesting future research endeavor would be to investigate whether the potential improvements to the ICM during the application process would yield any benefits for the companies used in the case studies.

References

Akkermans, D., van Ees, H.,Hermes, N.,Hooghiemstra, R., Van der Laan, G., Postma, T., & van Witteloostuijn, A. (2007). Corporate governance in the Netherlands: An overview of the application of the Tabaksblat Code in 2004. *Corporate Governance: An International Review*, 15, 1106–1118.

Alles, M. A., Kogan, A., & Vasarhelyi, M.A. (2002). Feasibility and economics of continuous assurance. *Auditing: A Journal of Practice & Theory, 21*(1), 125-138.

Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems, 7*(2), 137-161.

Alles, M.G., Kogan, A., & Vasarhelyi, M.A. (2008b). Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems, 22*(2), 195-214.

Alles, M.G., Kogan, A., & Vasarhelyi, M.A. (2009). *Principles and Problems of Audit Automation as a Precursor to Continuous Auditing.* Unpublished working paper, Rutgers Business School.

Alles, M.G., Kogan, A., Vasarhelyi, M.A., & Wu, J. (2008a). *Continuous Data Level Auditing Using Continuity Equations*. Unpublished working paper, Rutgers Business School.

Ashbaugh-Skaife, H., Collins, D.W., & Kinney, W.R. (2007). The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. *Journal of Accounting and Economics, 44*(1), 166-192.

Baker, R., Bealing Jr., W. E., Nelson, D. A., & Blair Staley, A. (2006). An Institutional Perspective of the Sarbanes-Oxley Act. *Managerial Auditing Journal, 21*(1), 23-33.

Bandilla, W., Bosnjak, M., & Altdorfer, P. (2003). Survey Administration Effects? A Comparison of Web Based and Traditional Written Self Administered Surveys Using the ISSP Environment Module. *Social Science Computer Review, 21*(2), 235–243.

Barribal, K.L., & While, A. (2006). Collecting data using a semi-structured interview: a discussion paper. *Journal of Advanced Nursing, 19*(2), 328-335.

Basten, A.R.J. (2004). De invloed van automatisering op AO/IC. Retrieved August 15, 2012 from http://www.compact.nl/artikelen/C-2004-3-Basten.htm

Boccasam, P.V., & Kapoor, N. (2003). Managing Separation of Duties Using Continuous Monitoring, IT Audit, 6. The Institute of Internal Auditors, Retrieved 4 September, 2012 from http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5433.

Bonnie, K.K., & Watson, M. W. (2009). SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and Information Technology. *Journal of Information Systems, 23*(2), 1-23.

Borthick, A.F., Jones, D.R., & Kim, R. (2001). Developing Database Query Proficiency: Assuring Compliance for Responses to Web Site Referrals. *Journal of Information Systems, 15*(1), 35-56.

Brau, J.C., & Fawcett , S.E. (2006). Initial Public Offerings: An Analysis of Theory and Practice. *Journal of Finance, 61*(1), 399-436.

Brinkkemper, S., Saeki, M., & Harmsen, F. (1999). Meta-modelling based assembly techniques for situational method engineering. *Information Systems, 24*(3), 209-228.

Brown, C. E., Wong, J. A., & Baldwin, A. A. (2006). Research streams in continuous audit: A review and analysis of the existing literature. In *Collected Papers of the Fifteenth Annual Research Workshop on: Artificial Intelligence and Emerging Technologies in Accounting, Auditing and Tax*, 123–135. Washington, D.C.

Brown, C.E., Wong, J., & Baldwin, A.A. (2007). A review and analysis of the existing research streams in continuous auditing. *Journal of Emerging Technologies in Accounting*. *4*(1), 1-28.

Brown, W. & Nasuti, F. (2005). What ERP systems can tell us about Sarbanes-Oxley. *Information Management & Computer Security, 13*(4), 311–327.

Cadbury Committee (1992). Report of the Committee on the Financial Aspects of Corporate Governance (Gee and Co., London).

Cangemi, M. P. (2011). *The Benefits of Continuous Monitoring*. New Jersey: Financial Executives Research Foundation.

Carney, W.J. (2006). The costs of being public after Sarbanes-Oxley: The irony of 'going private'. *Emory Law Journal* , 55, 141-160.

Chan, D.Y., & Vasarhelyi, M.A. (2011). Innovation and Practice of Continuous Auditing. *International Journal of Accounting Information Systems 12*(2), 152-160.

Chan, S. (2004). Sarbanes-Oxley: the IT dimension. *The Internal Auditor, 61*(1), 31-3.

Chen S. (2003). Continuous Auditing: Risk, Challenges and Opportunities. *International Journal of Applied Management and Technology*, *1*(1).

Chen Y. (2004). Continuous Auditing using Strategic-system approach. *Internal Auditing*, *19*(3), 31-36.

CICA/AICPA (1999). Research Report on Continuous Auditing. *Research Report, Toronto, Canada: The Canadian Institute of Chartered Accountants*.

Coderre, D. (2006). A Continuous View of Accounts. *Internal Auditor, April, 63*(2), 25-31.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (1992). Internal Control - Integrated Framework, Volume 2, American institute of Certified Publix Accountants, Jersey City, N. J.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004). Enterprise Risk Management - Integrated Framework. AICPA, New Jersey.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2008). Guidance on monitoring internal control systems. Retrieved April 1, 2012 from http://www.coso.org/guidance.htm

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2011). Enterprise Risk Management - Integrated Framework, Draft for Public Exposure. AICPA, New Jersey.

Corbetta, P. (2003). *Social Research: Theory, Methods and Techniques*. London: Sage Publications.

Daigle, J.J., Daigle, R.J., & Lampe, J.C. (2008). Auditor Ethics for Continuous Auditing and Continuous Monitoring. *Information Systems Control Journal*, 3.

Damianides, M. (2005): Sarbanes–Oxley and IT Governance: New Guidance on IT Control and Compliance. *Information Systems Management, 22*(1), 77-85.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism. *Information Systems Journal, 8*(4), 273-289. Willey Online Library.

Dassen, R., Maijoor, S.J., & Wallage, Ph. (2002). *Control & Assurance,* Reed Business Information.

de Bruijn, R.J.C.H.M., & op het Veld, M.A.P. (2008). Benchmarking IT application controls. Retrieved August 15, 2012, from www.compact.nl/pdf/C-2008-3-Bruijn.pdf

Debreceny, R.S. (2006). Re-engineering IT Internal Controls - Applying capability Maturity Models to the Evaluation of IT Controls. Proceedings of the 39th Hawaii International Conference on System Sciences.

Doyle, J., Ge, W., & S. McVay (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics,* 44, 193-223.

Dull, R.B., Tegarden, D.P., & Schleifer, L.L.F. (2006). ACTVE: A Proposal for an Automated Continuous Transaction Verification Environment. *Journal of Emerging Technologies in Accounting, 3*(1), 81-96.

Elliott, R. K. (2002). Twenty-First Century Assurance, *Auditing: A Journal of Practice and Theory, 21*(1), 139-146.

European Commission (2004). Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments. Brussels: Official Journal of the European Union L 145 30.04.2004, 1-44.

Financial Accounting Standard Board (FASB) (1975). Accounting for Contingencies. Statement No. 5. Stamford, CT: FASB.

Flowerday, S., Blundell, A.W., & Von Solms, R. (2006). Continuous auditing technologies and models: A discussion. *Computers & Security, 25*(5), 325-331.

Fox, C. & P. Zonneveld (2003). *IT Control Objectives for Sarbanes–Oxley.* Rolling Meadows, IL: IT Governance Institute.

Fox, C., & Zonneveld, P. (2006). *IT control objectives for Sarbanes-Oxley: The role of IT in the design and implementation of internal control over financial reporting* (2nd ed.). Rolling Meadows, IL: IT Governance Institute.

Garland, R. (1991). The mid-point on a rating scale: is it desirable? *Marketing Bulletin,* 2, 66–70.

Gartner (2009). Continuous Controls Monitoring for Transactions: The Next Frontier for GRC Automation. Report ID: G00164382.

Ge, W., & McVay, S. (2005). The Disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizon, 19*(3), 137-158.

Gillan, S. (2006). Recent developments in corporate governance: An overview. Journal of Corporate Finance, 12, 381-402.

Gillan, S.L., & Starks, L.T. (1998). A survey of shareholder activism: motivation and empirical evidence. *Contemporary Finance Digest, 2* (3), 10-34.

Goergen, M., Manjon, M.C., & Renneboog, L. (2008). Recent developments in German corporate governance. *International Review of Law and Economics, 28*(3), 175-193.

Gordon, L., Loeb, M., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy,* 25, 503-530.

Greenstein, M.M., & Ray, A. W. (2002). Holistic, Continuous Assurance Integration: e-Business Opportunities and Challenges, *Journal of Information Systems, 16*(1:Supplement), 1-20.

Groomer, S.M., & Murthy, U.S. (1989). Continuous Auditing of Database Applications: An Embedded Audit Module Approach. *Journal of Information Systems, 3*(2), 53-69.

Groomer, S.M., & Murthy, U.S. (2003). Monitoring high-volume online transaction processing systems using a continuous sampling approach. *International Journal of Auditing, 7*(1), 3-19.

Gupta, P., & Thomson, J.C. (2006). Use of COSO 1992 in management reporting on internal control. *Strategic Finance,* 27-33.

Hall, B.H., & Khan, B. (2003). Adoption of new technology, *Working paper E03-330,* Berkeley, University of California.

Hall, J.A. & Liedtka, S.L. (2007). The Sarbanes-Oxley Act: implications for large-scale IT outsourcing. In: Communications of the ACM, 50(3), 95-100.

Handscombe, K. (2007). Continuous Auditing From a Practical Perspective. *Information Systems Control Journal,* 2.

Hass, S., Abdolmohammadi, M.J. & Burnaby, P. (2006), The Americas literature review on internal auditing. *Managerial Auditing Journal, 21*(8), 835-844.

Henrickson, R. (2009). Practitioner Discussion of Principles and Problems of Audit Automation as a Precursor for Continuous Auditing. University of Waterloo Centre for Information Integrity and Information Systems Assurance 6th Bi-Annual Research Symposium. Toronto.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information System Research. *MIS Quarterly*. *28*(1), 75-105.

Huffman, A, & Grump, J. (2005). Applying Continuous Controls Monitoring for Achieving Compliance and Business improvement. *Financial Executive, 21*(8), 54-56.

Hunt, R., & Jackson, M. (2010). An introduction to continuous controls monitoring. *Computer Fraud & Security*, Sid. 16-19.

Hunton, J., Wright, A., & Wright, S. (2002). Assessing the Impact of More Frequent External Financial Statement Reporting and Independent Auditor Assurance on Quality of Earnings and Stock Market Effects. Working paper presented at the Fifth Continuous Auditing Symposium.

ISACA Standards Board (2002). Continuous Auditing: Is It a Fantasy or a Reality? *Information Systems Control Journal, 5*, 43-46.

ISO, ISO/IEC 27002 (2005). Information technology - Security techniques - Code of practice for information security management. Retrieved August 15, 2012, from http://www.iso.org/iso/catalogue_detail?csnumber=50297

Kaarst-Brown, M. and Kelly, S. (2005). IT governance and Sarbanes-Oxley: the latest sales pitch or real challenges for the IT function? *Proceedings of the 38th Hawaii International Conference on System Scienc*es – 2005, IEE.

Kajornboon, A. B. (2005). Using interviews as research instruments. *E-Journal for Research Teachers, 2*(1).

Kinney, W. (2000). Research opportunities in internal control quality and quality assurance. Auditing 19, 83–90.

Kneer, D.C. (2003). Continuous Assurance: We are Way Overdue. *Information System Control Journal*, 1.

Kogan, A., Sudit, E.F., &Vasarhelyi M.A. (1999). Continuous online auditing: A program of research. *Journal of Information Systems,* 87-103.

Krishnan, J. (2005). Audit committee quality and internal control: an empirical analysis. The Accounting Review, 80, 649-675.

Kuhn, J.R., & Sutton S.G (2010). Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems,* 24, 91-112.

Kuhn, J.R., & Sutton, S.G. (2006). Learning from WorldCom: Implications for fraud detection through continuous assurance. *Journal of Emerging Technologies in Accounting,* 3, 61-80.

Kvale, S., & Brinkmann, S. (2009). *InterViews: Learning the Craft of Qualitative Research Interviewing*. (V. Knight, S. Connelly, L. Habib, A. Virding, & J. Robinson, Eds.)*Evaluation and Program Planning* (Vol. 20, p. 354). Sage Publications.

Lainhart , J.W. (2000). COBIT: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities. Journal of Information Systems.

Lamm, J., Blount, S., Cooper, N., Camm, M., Boston, S., Cirabisi, R., Handal, K., McCracken, W., Datskovsky, G., Fox, C., Zanella, R., Scheil, H., Meyer, J., & Srulowitz, A. (2010). *Under Control: Governance Across the Enterprise.* New York, NY: Springer-Verlag.

Larsen, M. H., Pedersen, M.K., & Andersen, K.V. (2006). IT Governance – Reviewing 17 IT Governance Tools and Analyzing the Case of Novozymes A/S. *Proceedings of the 39th Hawaii International Conference on System Sciences*.

Lehman, C., Ramamoorti, S., & Watson, M. (2010). Maximized Monitoring. *Internal Auditor,* 56-59.

Li, S.H, Huang, S.M., & Lin, Y.C. (2007). Developing a continuous auditing assistance system based on information process models. *Journal of Computer Information Systems*.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. (A. Barazini, J. Ramirez, C. Schaerer, & P. Thalmann, Eds.) *Decision Support Systems, 15*(4), 251-266. Elsevier.

McClean, C., Balaouras, S., & Hayes, N. (2011). The Forrester Wave™: Enterprise Governance, Risk, And Compliance Platforms, Q4 2011. Forrester Research. Retrieved August 15, 2012, from http://www.forrester.com/The+Forrester+Wave+Enterprise+Governance+Risk+And+Compliance+Platforms+Q4+2011/fulltext/-/E-RES57692

Messick, S. (1989). Validity. In R. L. Linn (Ed.), *Educational measurement*. Washington, DC: American Council on Education and National Council on Measurement in Education.

Mills, D., Call, W., & Drew, A. (2000). *Foundations of Accounting*. Sydney: UNSW Press.

Moeller, R. R. (2005). Brink's Modern Internal Auditing, 6th edition, John Wiley & Sons, New York.

Morris, J.J. (2011). The Impact of Enterprise Resource Planning (ERP) Systems on the Effectiveness of Internal Controls over Financial Reporting. *Journal of Information Systems, 25*(1), 129-157.

Murthy, U.S. (2004). An Analysis of the Effects of Continuous Monitoring Controls on e-Commerce System Performance. *Journal of Information Systems, 18*(2), 29-47.

Nehmer, R. (2003). Continuous Audits: Taking the Plunge. *Information Systems Control Journal*, 1.

Nelson L. (2004). Stepping into Continuous Audit: a health-care audit shop shares its strategy for making real-time auditing a success. *Internal Auditor*, *6*(2), 27-29.

Nigrini, M.J., & Johnson, A.J. (2008). Using Key Performance Indicators and Risk Measures in Continuous Monitoring. *Journal of Emerging Technologies in Accounting*, *5*(1), 65-80.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts Working Papers on Information Systems, 10*(26), 1-49.

Pagano, M., Panetta, F., & Zingales, L. (1998), Why do computers go public? An empirical analysis, *Journal of Finance* 53, 27–64.

Pathak J., Chaouch B., & Sriram R.S. (2005). Minimizing Cost of Continuous Audit: Counting and Time dependent strategies. *Journal of Account and Public Policy, 24*(1), 61-69.

Payment Card Industry (2010). PCI DSS Requirements and Security Assessment Procedures. PCI Data Security Standard version 2.0. Retrieved August 15, 2012, from https://www.pcisecuritystandards.org

Potla, L. (2003). Detecting Accounts Payable Abuse Through Continuous Auditing. IT Audit, 6. Retrieved 4 September, 2012 from http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5458.

Public Company Accounting Oversight Board (PCAOB) (2004). *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements.* Auditing Standard No. 2. Washington, D.C.: PCAOB.

Public Company Accounting Oversight Board (PCAOB) (2010). *Audit Evidence.* Auditing Standard No. 15. Washington, D.C.: PCAOB.

Racz, N., Weippl, E., & Seufert, A. (2010). A frame of reference for research of integrated governance, risk, and compliance (GRC). In: Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (2010).

Ramos, M. (2004). How to Comply with Sarbanes-Oxley Section 404. Wiley, Hoboken, NJ.

Rezaee, Z., Ford, W., & Elam, R. (2000). Real-Time Accounting Systems, *Internal Auditor, 57*(2), 62-67.

Rezaee Z., & Hoffman, C. (2001). XBRL: standard electronic financial reporting. *Internal Auditor*, 46-51.

Rezaee, A., Elam, R., & Sharbatoghlie, A. (2002). Continuous auditing: Building automated auditing capability. *Auditing: A Journal of Practice & Theory* 21 (Spring): 147–163.

Rezaee, Z. (2005). Causes, consequences, and deterrence of financial statement fraud. *Critical Perspectives on Accounting*, *16*(3), 277-298.

Rikhardsson, P., Best, P., & Juhl-Christensen, C. (2006). Sarbanes-Oxley compliance, internal control, and ERP systems: the case of mySAP ERP. In: Ferran, C., Salim, R. (Eds.), Enterprise Resource Planning for Global Economies: Managerial Issues and Challenges, Ch. 12, Hershey, New York.

Root S. J. (1998). Beyond COSO: Internal Control to Enhance Corporate Governance. First edition. New York: John Wiley and Sons Inc.

Rose, W.C., & Hirte, B. (1996). Carolina Power and Light: Smart Auditing. In: *Enhancing Internal Auditing Through Innovative Practices*, edited by G. L. Gray, and M. J. Gray, 47–57. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Runeson, P., & Hoest, M. (2008) Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering, 14*(2), 131-164. Kluwer Academic Publishers.

Searcy, D.L., & Woodroof, J.B. (2003a). Continuous Auditing: Leveraging Technology. *The CPA Journal, 73*(5), 46-48.

Searcy, D., Woodroof, J., & Behn, B. (2003b). Continuous Audit: The motivations, benefits, problems, and challenges identified by partners of a Big 4 Accounting Firm.

Securities and Exchange Commission (SEC) (2003). Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. Retrieved August 23, 2012, from http://www.sec.gov/rules/final/33-8238.htm#P203_51386

Securities and Exchange Commission (SEC) (2007). Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934. Retrieved August 23, 2012, from http://www.sec.gov/rules/interp/interparchive/interparch2007.shtml

Senft, S., & Gallegos, F. (2009). *Information Technology Control and Audit*, 3rd Ed. Boca Raton, FL: Auerbach Publications.

Shaw, B. (2005). Bill C198-Sarbanes-Oxley Comes for Canada. Bill 198-Sarbanes-Oxley comes to Canada. Retrieved 15 August, 2012 from http://www.itprojecttemplates.com/WP_SEC_BillC198.htm

Shleifer, A., Vishny, R., 1997. A survey of corporate governance. Journal of Finance 52, 737–775.

Simmons, M. R. (1997). COSO based auditing. *The Internal Auditor, 54*(6), 68-73.

Simons R. (2000). Performance Measurement & Control systems for implementing strategy: text and cases, Prentice Hall: New Jersey.

Singleton, T. (2003). The Ramifications of Sarbanes-Oxley. *Information Systems Control Journal*, 3, 11-16.

Singleton, T., & Singleton, A.J. (2005). Auditing Headaches? Relieve Them with CAR. *The Journal of Corporate Accounting & Finance*, 17-27.

Starreveld, R., de Mare, B., & Joels, E. (1994). *Bestuurlijke Informatieverzorging*, Vol. 1, Samsom, Alphen aan den Rijn, 4th edition.

Swartz, N. (2003). The cost of Sarbanes-Oxley. *Information Management Journal, 37*(5), 8.

Takeda, H., Veerkamp, P., Tomiyama, T., & Yoshikawa, H. (1990). Modeling design processes. *AI Magazine*, 11(4), 37–48.

Taylor, M., & Murphy, A. (2004). SMEs and E-business. *Journal of Small Business and Enterprise Development, 11*(3),280-289.

Teeter, R., & Brennan, G. (2008). *Aiding the Audit: Using the IT Audit as a Springboard for Continuous Controls Monitoring,* Unpublished working paper, Rutgers Business School.

Teeter, R., Alles, A., & Vasarhelyi, M.A. (2010). *Remote Audit: A Research Framework*. Unpublished working paper, Rutgers Business School.

The Securities and Exchange Commission (SEC) (2002). Sarbanes – Oxley Act of 2002. Washington, DC, USA.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence informed management---knowledge by means of Systematic review. *British Journal of Management*, 207-222.

Turoff, M., Chumer, M., Hiltz, S.R., Klashner, R., Alles, M.G., Vasarhelyi, M.A., & Kogan, A. (2004). Assuring Homeland Security: Continuous Monitoring, Control & Assurance of Emergency Preparedness. *Journal of Information Technology Theory and Application, 6*(3), 1-24.

Tuttle, B., & Vandervelde, S.D. (2007). An empirical examination of COBIT as an internal control framework for information technology. *International Journal of Accounting Information Systems, 8*(4), 240-263.

U.S. Congress (2002). An act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. The Sarbanes-Oxley Act, 107th Cong., H.R. 3763.

Vaishnavi, V., & Kuechler, W. (2007). *Design science research methods and patterns: innovating information and communication technology*. Boca Raton, Florida: Auerbach Publications.

Valipour, H., Moradi, J., & Fatheh, M.H. (2012). The Impact of Enterprise Resource Planning (ERP) on the Internal Controls Case Study: Esfahan Steel Company. *European Journal of Social Sciences 28*(2), 228-238.

Vasarhelyi, M.A., & Halper, F.B. (1991). The continuous audit of online systems. *Auditing: A Journal of Practice and Theory, 10*(1).

Vasarhelyi, M. A., Kogan, A., & Alles, M. G. (2002). Would Continuous Auditing Have Prevented The Enron Mess?, *CPA Journal (The), 72*(7), 80.

Vasarhelyi, M. A., & Greenstein, M. L. (2003). Underlying Principles of the Electronization of Business: A Research Agenda, *International Journal of Accounting Information Systems, 4*(1), 1-25.

Vasarhelyi, M.A., Alles, M.G. & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting* 1, 121.

Vasarhelyi, M.A., Kuenkaikaew, S., Littley, J., & Williams, K. (2008). Continuous Auditing Technology Adoption in Leading Internal Audit Organizations. *Journal of Information Systems*.

Vasarhelyi, M.A., Alles, M., Kuenkaikaew, S., & Littley, J. (2012). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International Journal of Accounting Information Systems, 13*, 267-281.

Warren, J.D., & Parker, X.L. (2003) .Continuous Auditing: Potential for Internal Auditors. *The Institute of Internal Auditors Research Foundation*.

Webster, J., & Watson, R. T. (2002). nalyzing the past to prepare for the future: writing a literature review. Management Information Systems Quarterly 26(2), xiii–xxiii.

Weerd, I. van de, & Brinkkemper, S. (2008). Meta-modeling for situational analysis and design methods. In M.R. Syed and S.N. Syed (Eds.), *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications,* 38-58. Hershey: Idea Group Publishing.

White, L. (2005). Does Internal Control Enhance or Impede, *Strategic Finance, 86*(8), 6-7.

Wier, B., Hunton, J., & HassabElnaby, H.R., (2007). Enterprise resource planning systems and non-financial performance incentives: The joint impact on corporate performance. *International Journal of Accounting Information Systems, 8*(3), 165-190.

Woodroof, J., & Searcy, D. (2001a). Audit Implications of Internet Technology: Triggering Agents over the Web in the Domain of Debt Covenant Compliance, Hawaii International Conference on System Sciences, 34th, HICSS, Hawaii.

Woodroof, J., & Searcy, D. (2001b). Continuous Audit: Model Development and Implementation within a Debt Covenant Compliance Domain. *International Journal of Accounting Information Systems, 2*(3), 169-191.

Yin, R. K. (1984). *Case study research: Design and methods.* Newbury Park, CA: Sage.

Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

Zhao N., Yen D.C., & Chang I.C. (2004). Auditing in the e-commerce era", *Information Management and Computer Security*, *12*(5), 389-399.

Zingales, L. (1998). Corporate governance. In: Newman, P. (Ed.). The New Palgrave Dictionary of Economics and the Law.

APPENDIX A. E-mail Request

Dear Mr./Mrs.,

As part of my graduation project in the Master of Business Informatics at Utrecht University, the Netherlands, this **online questionnaire** aims at identifying the perceived **benefits** that the implementation of a **Continuous Monitoring tool** will bring to organizations around the world. Therefore, I would like to ask you to participate in a short questionnaire that asks you to rate a series of benefits, depending on your area of expertise.

Professionals from the Internal Control, Internal Audit, External Audit, Business Process Management, Risk Management, Financial Control and SOX Compliance teams are targeted. As every answer is very important for the success of this research, it would be very much appreciated if you could **forward this request to your colleagues** that work in the above mentioned areas as well. The responses of this questionnaire will be treated **confidentially**.

The questionnaire consists of three pages and should only take about **10 minutes** or less of your time, depending on your areas of expertise. If you have any questions about the survey, please feel free to email: R.Turtoi@students.uu.nl.

The questionnaire can be reached via this URL:
http://contmonitoring.limequery.org/63131/lang-en

Note: In order to involve as many professionals as possible, the sum of **€ 1,00** will be **donated** by the research team to the **DiDi charitable foundation** www.didifoundation.nl for the **first 200 complete responses**.

Thank you for your time!

Kind regards,

Razvan Turtoi
Master student Business Informatics

Utrecht University

The Netherlands

APPENDIX B. LinkedIn Groups

Accounting & Control Professionals in Nederland
Certified ISO27000 Lead Auditor
CIPFA – the Chartered Institute of Public Finance and Accountancy
Continuous audit
Continuous Controls Monitoring
Deloitte Audit
Deloitte Consulting
Enterprise Risk Management Association
Finance Club
GE (General Electric)
Governance, Risk & Compliance
Governance, Risk & Compliance (GRC) Professionals
Governance, Risk and Compliance Management (GRC)
IIA Nederland
Information Security Community
Internal Audit & Risk Consultants
Internal Audit Consultants Network
Internal Audit/SOX Group
Internal Control Worldwide Network
ISACA - IT Governance Professionals
IT audit
Linked: Energy (Energy industry expertise)
Official - Certified Internal Auditor (CIA)
Official – Certification in Risk Management Assurance (CRMA)
Operational Risk & Regulation
PricewaterhouseCoopers LLP (PwC US)
PwC Consulting Professionals Network
Sarbanes Oxley (SOX)
Sarbanes Oxley Consultants
SOX International Group
SOX Professionals Group Lk-in
The Institute of Internal Auditors (Official Global Group)
The Institute of Risk Management
Big Four Accounting Consulting - Deloitte, Ernst & Young, KPMG, PwC, Accenture, Capgemini (Big4.com)
Solvency 2 Experts Group
ISO 31000 Risk Management Standard

APPENDIX C. Newsletter NBA

In welke mate heeft het gebruik van een Continuous Monitoring tool voordeel voor organisaties?

Het gebruik van een tool voor het doorlopend monitoren van de werking van interne controles zou veel voordelen opleveren, van een besparing op de accountantskosten tot een verhoging van de kwaliteit van de interne en externe audit. Wat is uw mening daarover? Deze vraag wordt u gesteld door Razvan Turtoi, in het kader van zijn afronding van de masteropleiding bedrijfsinformatica aan de Universiteit van Utrecht. Open enquête »

NEDERLANDSE BEROEPSORGANISATIE VAN ACCOUNTANTS (NBA) [15]

[15] http://nba.m17.mailplus.nl/genericservice/code/servlet/React?encId=YTIMebpAv79mmbD&actId=41895&command=openhtml

APPENDIX D. Online Questionnaire (1)

Welcome!

As part of my graduation project in the Master of Business Informatics at Utrecht University, the Netherlands, this questionnaire aims at identifying the perceived benefits that the implementation of a **Continuous Monitoring tool** will bring to organizations around the world. All professionals from the Internal Control, Internal Audit, External Audit, Business Process Management, Risk Management, Financial Control and SOX Compliance teams are invited to participate.

Continuous Monitoring (CM) represents a business management monitoring process with the ability to ensure that the internal controls function as intended and transactions operate properly. Furthermore, ***Gartner (2010)*** *defines* ***continuous monitoring*** *as the use of control automation to lower the risks of fraud and strengthen financial governance. CM increases the trustworthiness of the controls, and increases the execution of managerial policies, and the operational effectiveness and efficiency for business processes and transactions*.

One specific **example** where CM can help is in the **Segregation of Duties** (SOD) area. Assume a user has the rights to enter suppliers and accounts payable invoices in the system. This would mean that this user could enter a fictitious supplier and a related invoice linked to that supplier, which may allow the user to commit fraud. At the moment, System Settings Access Rights checks are done manually and are very labor-intensive. Through CM, automated SOD scans are being performed on a regular basis to flag the inappropriate behavior as soon as it happens.

Another **example** is the **three-way match**. It avoids payment for goods that have not been received yet, but for which the supplier has provided an invoice. In order for the payment to be made, the purchase order has to match the supplier's invoice and the receipt record for the goods that were delivered. Often, this rule is overridden, and the payment is blocked. In case the three-way match is turned off, fraud can take place. Through CM, scans are being performed on all the transactions that take place and alerts are sent to the necessary people on a timely-manner in the event the three-way match was bypassed.

The questionnaire consists of three pages and should only take about **10 minutes** or less of your time depending on your areas of expertise. If you have any questions about the survey, please feel free to email: R.Turtoi@students.uu.nl .

Note: In order to involve as many professionals as possible, the amount of **€1,00** will be **donated** by the research team to the **DiDi charitable foundation** www.didifoundation.nl for the **first 200 complete response**.

Thank you for your time!

Kind regards,
Razvan Turtoi
Master student Business Informatics

Utrecht University
The Netherlands

APPENDIX D. Online Questionnaire (2)

1 [Q001]

Please choose your areas of expertise:

*

Please choose **all** that apply:

- ☐ Business Owners (Internal Controllers, Risk Management, Financial Controllers, etc.):
- ☐ Internal Auditor
- ☐ External Auditor

Please note that if **one area** is chosen, than only statements regarding that area will appear on the next page. In case **more than one area** are selected, then **different sets** of statements that belong to **each individual area** will have to be answered.

2 [Q002]How many years of professional experience do you have in the above mentioned area(s)? *

Please choose **only one** of the following:

- ○ Less than 1 year
- ○ 1+ years
- ○ 2+ years
- ○ 5+ years
- ○ 7+ years
- ○ 10+ years
- ○ More than 15 years

3 [Q003]What department are you working in?

Please write your answer here:

4 [Q004]What is the size of the team you are part of?

Please write your answer here:

APPENDIX D. Online Questionnaire (3)

5 [Q005]What type of regulations does your team have to assure compliance to?

Please write your answer here:

Provide where applicable.

6 [Q006]What sector does your organization operate in?

Please write your answer here:

Provide where applicable.

7 [Q011]

Please rate each affirmation below based on your experience as a BusinessOwner (Internal Control, Risk Management, Financial Control, etc.).

(1 – Strongly Disagree, 2 – Disagree, 3 – Agree, 4 – Strongly Agree)

Continuous Monitoring of internal controls will:

*

Only answer this question if the following conditions are met:
° ((**Q001_SQ001.NAOK** == "Y"))

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Agree	Strongly Agree
decrease the stress level of business owners during an audit.	○	○	○	○
increase the quality of business decisions.	○	○	○	○
help business owners focus on the risk areas that are critical for reaching the established objectives.	○	○	○	○
reduce the amount of time the staff needs for monitoring the controls.	○	○	○	○
increase the likelihood of capturing at an early stage fraudulent and abusive actions.	○	○	○	○
increase the operational performance of the business, e.g. by detecting, at an early stage, duplicate payments, misapplied warranties, incorrect discounts.	○	○	○	○
improve the awareness level by analyzing all the transactions on a real-time basis.	○	○	○	○
increase the system security assurance level by detecting in real-time unauthorized access and manipulation of sensitive data.	○	○	○	○
help in better identifying the opportunities for process improvements.	○	○	○	○
decrease the amount of financial loss through ongoing monitoring of purchases, payments, payroll, and travel & entertainment expenses.	○	○	○	○
improve the internal control framework quality, e.g. reducing the number of controls by merging two controls into one.	○	○	○	○
increase the focus on measuring the quality of processes and data.	○	○	○	○

APPENDIX D. Online Questionnaire (4)

8 [Q012]

Please rate each affirmation below based on your experience as an Internal Auditor.

(1 – Strongly Disagree, 2 – Disagree, 3 – Agree, 4 – Strongly Agree)

Continuous Monitoring of internal controls will:

*

Only answer this question if the following conditions are met:
° ((**Q001_SQ002.NAOK** == "Y"))

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Agree	Strongly Agree
increase the reliability of financial statements through ongoing monitoring of financial transactions.	○	○	○	○
increase the transparency of the financial information provided to the shareholders.	○	○	○	○
provide a complete view of the effectiveness of all the transactions for which controls are set in place.	○	○	○	○
increase the time spent on hard-to-test manual controls.	○	○	○	○
decrease the amount of staff needed for audit.	○	○	○	○
decrease the travel time needed for audits in multi-national organizations.	○	○	○	○
decrease the costs for compliance.	○	○	○	○
decrease the risk of non-compliance, which leads to penalties being issued by regulatory organizations.	○	○	○	○
decrease the amount of stress of the internal audit team.	○	○	○	○
level the amount of work throughout the whole year, rather than period-end close.	○	○	○	○
increase the reliability of the audit results, e.g. accuracy of financial reports.	○	○	○	○
improve the quality of the internal audit by providing better audit evidence and scoping on the most important indicators, thus a more thorough audit trail.	○	○	○	○
ensure that the internal audit team will be better prepared for the external audit.	○	○	○	○
decrease the number of reporting follow-ups by reducing the amount of accounting errors that lead to manual follow-ups and time-consuming examinations.	○	○	○	○
reduce the time required for evaluating the effectiveness of controls due to higher accessibility to work papers and reports provided by the business.	○	○	○	○
provide the change from compliance-oriented audits to risk identification and process improvement-oriented audits.	○	○	○	○

APPENDIX D. Online Questionnaire (5)

9 [Q013]

Please rate each affirmation below based on your experience as an External Auditor.

(1 – Strongly Disagree, 2 – Disagree, 3 – Agree, 4 – Strongly Agree)

Continuous Monitoring of internal controls will:

*

Only answer this question if the following conditions are met:
° ((**Q001_SQ003.NAOK** == "Y"))

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Agree	Strongly Agree
increase the reliance on the work of the internal audit team.	○	○	○	○
increase the efficiency of the review of the internal audit trail.	○	○	○	○
increase the quality of the audit.	○	○	○	○
increase the reliability of the audit.	○	○	○	○
decrease the time required for testing the controls.	○	○	○	○
decrease the audit fees that external auditors request to perform an audit.	○	○	○	○
decrease the travel time for external auditors.	○	○	○	○
decrease the likelihood of future litigations.	○	○	○	○
decrease the likelihood of rushing the audit to meet the examination deadlines.	○	○	○	○
provide external audit firms the necessary capabilities to match the increase in complexity of future markets.	○	○	○	○

10 [Q025]What types of risk assessment frameworks are you using in your organization?

Please write your answer here:

Current and past.

11 [Q023]Please state which, in your opinion, are the most important types of internal controls inside organizations (financial, operational, etc.).

Please write your answer here:

APPENDIX D. Online Questionnaire (6)

12 [Q021]

Please provide an estimation of the average state of internal controls identified in your organization/the industry.

Please choose **all** that apply and provide a comment:

☐ Manual detective	
☐ Manual preventive	
☐ Automated detective	
☐ Automated preventive	
Other:	

Please provide the approximate percentage.

13 [Q022]What would be the challenges, in your opinion, encountered when evolving from manual assurance techniques to Continuous Monitoring technology?

Please write your answer here:

14 [Q024]If you would like to receive the results of this survey, please provide your e-mail address below:

Please write your answer here:

APPENDIX E. Online Questionnaire Results (1)

Results for Business Owners

Nr.	Continuous Monitoring will:	Mean	Std. Dev.
3.	Help business owners focus on the risk areas that are critical for reaching the established objectives.	3,357	0,577
6.	Increase the operational performance of the business, i.e. by detecting, at an early stage, duplicate payments, misapplied warranties, incorrect discounts.	3,333	0,612
12.	Increase the focus on measuring the quality of processes and data.	3,333	0,57
5.	Increase the likelihood of capturing at an early stage fraudulent and abusive actions.	3,286	0,673
1.	Decrease the stress level of business owners during an audit.	3,238	0,821
9.	Help in better identifying the opportunities for process improvements.	3,214	0,645
10.	Decrease the amount of financial loss through ongoing monitoring of purchases, payments, payroll, and travel & entertainment expenses.	3,214	0,682
2.	Increase the quality of business decisions.	3,167	0,66
4.	Reduce the amount of time the staff needs for monitoring the controls.	3,143	0,814
7.	Improve the awareness level by analyzing all the transactions on a real-time basis.	3,143	0,683
8.	Increase the system security assurance level by detecting in real-time unauthorized access and manipulation of sensitive data.	3,143	0,647
11.	Improve the internal control framework quality, i.e. reducing the number of controls by merging two controls into one.	3,095	0,759

APPENDIX.E. Online Questionnaire Results (2)

Results for Internal Auditors

Nr.	Continuous Monitoring will:	Mean	Std. Dev.
1.	Increase the reliability of financial statements through ongoing monitoring of financial transactions.	3,413	0,617
12.	Improve the quality of the internal audit by providing better audit evidence and scoping on the most important indicators, thus a more thorough audit trail.	3,261	0,648
16.	Provide the change from compliance-oriented audits to risk identification and process improvement-oriented audits.	3,174	0,769
3.	Provide a complete view of the effectiveness of all the transactions for which controls are set in place.	3,109	0,795
11.	Increase the reliability of the audit results.	3,087	0,661
6.	Decrease the travel time needed for audits in multi-national organizations.	3	0,699
13.	Ensure that the internal audit team will be better prepared for the external audit.	3	0,596
15.	Reduce the time required for evaluating the effectiveness of controls due to higher accessibility to work papers and reports provided by the business.	3	0,699
8.	Decrease the risk of non-compliance, which leads to penalties being issued by regulatory organization.	2,978	0,683
10.	Level the amount of work throughout the whole year, rather than period-end close.	2,957	0,729
2.	Increase the transparency of the financial information provided to the shareholders.	2,804	0,778
7.	Decrease the costs for compliance.	2,804	0,719
14.	Decrease the number of reporting follow-ups by reducing the amount of accounting errors that lead to manual follow-ups and time-consuming examinations.	2,804	0,582
4.	Increase the time spent on hard-to-test manual controls.	2,761	0,874
5.	Decrease the amount of staff needed for audit.	2,739	0,681
9.	Decrease the amount of stress of the internal audit team.	2,283	0,584

APPENDIX.F. Online Questionnaire Results (3)

Results for External Auditors

Nr.	Continuous Monitoring will:	Mean	Std. Dev.
3.	Increase the quality of the audit.	3,375	0,5
2.	Increase the efficiency of the review of the internal audit trail.	3,313	0,602
4.	Increase the reliability of the audit.	3,313	0,479
1.	Increase the reliance on the work of the internal audit team.	3,25	0,577
10.	Provide external audit firms the necessary capabilities to match the increase in complexity of future markets.	3,063	0,574
5.	Decrease the time required for testing the controls.	2,875	0,619
9.	Decrease the likelihood of rushing the audit to meet the examination deadlines.	2,875	0,619
6.	Decrease the audit fees that external auditors request to perform an audit.	2,688	0,479
7.	Decrease the travel time for external auditors.	2,625	0,719
8.	Decrease the likelihood of future litigations.	2,563	0,512

APPENDIX E. Online Questionnaire Results (4)

Professional group	Challenges
Business Owners	• Identifying the right set of controls for monitoring, from an operational and financial point of view;
	• Business process reengineering: automation of controls;
	• Harmonization of ERP systems;
	• Cooperation across business and assurance functions;
	• Awareness, understanding and involvement by the business;
	• Mapping human business interpretation to a model that works with thresholds and weights;
	• Cultural change involved with the way alerts are communicated and handled: the manner systemic data is presented and translated into strategic change to optimize risk (loss) vs. cost (of monitoring);
	• Teach staff to focus on the outliers instead of controlling the whole bunch. Signaled outliers need to be followed up upon timely and correctly.
Internal Auditors	• Mind shift in internal control: requires a thorough insight in the data-models and processes;
	• Awareness, understanding and involvement by the business;
	• Technical capabilities of audit staff, or access to qualified technical staff outside the audit department;
	• Changing the testing mentality of the audit staff - educating auditors on the technology;
	• Focus on the outliers instead of controlling the entire population.
External Auditors	• Disperse IT environment;
	• Data interpretation of false positives;
	• Knowledge of IT landscape, systems and operation data quality;
	• Most critical is to monitor the right controls set, otherwise people will manipulate the results;
	• Ensure that these controls are relevant from an operational point of view as well as financial reporting, otherwise business will not pay attention to it;
	• Current assurance standards are outdated in reporting (once a year). This might have been effective during the 60's but not anymore. This has to shift to a more regular assurance period.
	• The biggest impact is on the change in the Quality Team work and then in management of the exceptions. The change is substantial and impacts on the approach, the risk organization structure and the external audit approach;
	• Automation of processes;
	• Mindset, education and experience in IT (tooling).

APPENDIX F. ICPT Detailed

Dimension No.	Dimension	Parameters	Additional explanations:
D1	Automation level	Automated Semi-automated Manual	What is the type of the control: automated, semi-automated, manual? **Automated:** the contorl is purely based on data extracted from the enterprise system, without any manual work. **Semi-automated:** the control is based on an exception report run within the enterprise system which requires a manual follow-up. **Manual:** the control is purely based on manual work.
D2	Control type	Preventive Detective	Is the control preventive or detective in nature? **Preventive controls** are proactive and form the first line of defense against erroneous manual inputs of data as they prevent errors and inconsistencies from occurring. **Detective controls** are meant to detect any errors and deviations from normal behavior after they have occurred.
D3	Frequency	Daily/weekly Monthly/quartely Annualy	How often would the control be tested during a CM implementation?
D4	Level of impact on key G/L accounts	High Medium Low	What is the level of impact on key General Ledger accounts when considering the materiality of transactions? Materiality is a concept related to the importance or significance of an amount or transaction. The threshold between high, medium and low are company/specific.
D5	ERP system knowledge	High Medium Low	This capability inquires whether for this control someone in the organization, i.e. financial/business controller, auditor or IT staff, has knowledge of the underlying system set-up such as tables, fields, etc.
D6	Root cause analysis	Yes No	Does the person who performs the control needs to be able to do a root cause analysis to make the control useful, e.g. drill-down, pivot tables, charting, trending and filtering?
D7	Manual intervention/adjustments of data	Yes No	Does the business process require manual intervention such as extra manual adjustments of payments after their approvals? Ex.: After a change in the enterprise system has been approved, i.e. on a purchase order, payment, etc., can a user perform other manual adjustments to that transaction before the order, payment, etc. is being released?
D8	Impact on Quality of Master Data (customer, item, pricing, supplier)	Yes No	Does the control focus on changes to the master data, i.e. changes to the limit amount of a payment, changes of bank accounts of existing vendors, adding fictitious vendors into the system, etc.