Continuous Auditing & Continuous Monitoring in a Broader Perspective

The Performance Management Potential of CA & CM

Master Thesis
K.H. (Koen) klein Tank
s0211931
University of Twente, the Netherlands & KPMG, the Netherlands

February 18, 2011

Contact

Author

Name: *Koen klein Tank*;
Student number: s0211931;
Function: Graduate University of Twente, KPMG, IT Advisory;
Address: Nieuwstraat 12, 7137 MJ, Lievelde, The Netherlands;
Phone: +31-62-467-7392;
Email: kleintank.koen@kpmg.nl.

Graduation Committee

First supervisor

Name: *Ton Spil*;
Function: Assistant Professor, Information Systems & Change Management;
Address: BBT University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands;
Phone: +31-53-489-3497;
Email: a.a.m.spil@utwente.nl.

Second supervisor

Name: *Pascal van Eck*;
Function: Assistant Professor, Information Systems Group, Department of Computer Science;
Address: BBT University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands;
Phone: +31-53-489-4648;
Email: p.a.t.vaneck@ewi.utwente.nl.

External supervisor

Name: *Menno Hoekstra*;
Function: Advisor KPMG, IT Advisory;
Address: Mr B.M. Teldersstraat 7, 6842 CT Arnhem, The Netherlands;
Phone: +31-26-389-9701;
Email: hoekstra.menno@kpmg.nl.

Management Summary

Most financial and auditing executives are aware of Continuous Auditing (CA) & Continuous Monitoring (CM) and of the general benefits of such approaches. Yet, relatively few organizations have realized their full potential, particularly at the enterprise-wide level. In many such initiatives costs can appear more certain than benefits. Thus, the business case for CA & CM can be difficult to make in traditional (ROI-based) monetary terms. Due to the complexity of most organizations and the ongoing focus on costs, there is an increased focus on adopting innovative ways to assess and manage risks while enhancing performance. This research shows the added value of Continuous Auditing (CA) & Continuous Monitoring (CM) for Performance Management (PM).

Conclusions & Recommendations Figure 1 illustrates the ideal theoretical situation in which enterprise-wide risk and performance management are integrated to keep performance and risk in balance, and in which CA & CM as technical assets contribute to this process.

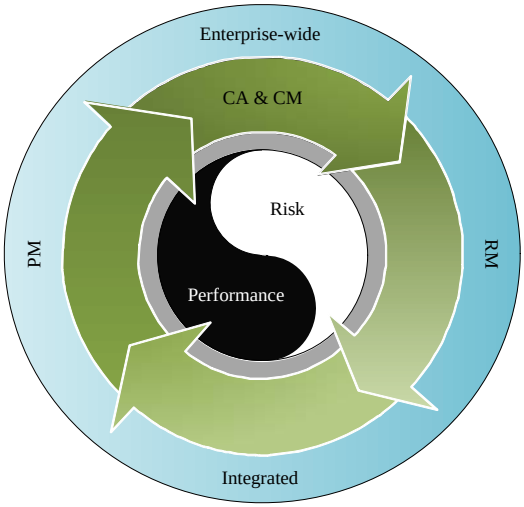

Figure 1: How CA & CM can add value to both, RM and PM

The premise here is to link CA & CM to Risk Management (RM) and PM. We think that if organizations want to succeed in today's environment, PM and RM should be performed in tandem (integrated) across the entire organization. These disciplines should not be performed as separate activities, they should be in balance as depicted in Figure 1. In this way, CA & CM can add value to both, thereby enabling the following benefits:

- ensure continuous reliability of performance and risk information;
- provide the management with accurate data and timely reporting of key risk and performance issues;

- analyze large volumes of transactions in less time, more automatically, more efficiently, and ultimately more cost-effective than using the traditional (snapshot) approach.

To reach these potential benefits, organizations should understand the extent to what they have to transform their performance and risks management approaches, controls, infrastructure, technology, and people:

- RM and PM should be applied in a strategic/integrated setting and across the entire organization. Organizations should take a systematic approach to RM and PM, e.g., following the COSO ERM - Integrated Framework and the Integral Framework for Performance Measurement;
- depending on the organization's industry and core risks, primary and secondary processes should be IT-facilitated;
- a minimum of 60 to 70 percent of controls should be automated and preventive in nature, with the balance being manual and detective;
- there should be standardized processes, systems, data and infrastructure;
- CA & CM activities should be centralized, thereby enabling that systems can be centrally monitored;
- there should be support from the C-level executives on all areas: CA & CM, RM and PM;
- responsibilities will shift, which require the auditors to create a broader understanding of the organization, and thereby, of its core processes, systems, objectives and risks.

The conclusions and recommendations are derived from literature, as well as from the practical information gained from interviews with three employees of Dutch organizations and three experts of KPMG.

Gaps Nevertheless, these interviews also revealed some gaps between the ideal situation as depicted in Figure 1 and the current practical situation in the organizations:

- the majority of the organizations do not have a centralized IT structure and information resides in too many places across the organization;
- in practice, the primary processes are not, or to a limited extent facilitated by a common IT system;
- at the greatest part of the organizations, the majority of the controls at the primary processes are manual;
- the greatest part of the organizations do not take a systematic, aggregated, and enterprise-wide approach to RM and PM;

- organizations are narrowly focusing on regulatory compliance, instead of taking a broader view on risk and performance management;
- the terminology used in practice to e.g., express control, risk, and performance indicators is very divergent.

Organizations should overcome these gaps and fulfill to the recommendations above, if they want to add value to PM. From this we conclude that an integrated approach to manage risks and performance with the help of CA & CM tooling, is about using the right information to achieve a meaningful view of risk across the enterprise, and to more accurately anticipate the associated impact on performance. In our opinion, creating value with CA & CM for PM is an opportunity in the sense that it makes it possible to sell CA & CM as a profit driver.

Further research There are some areas in which further research would significantly contribute to the findings described in this thesis:

- further research about RM and PM methods/frameworks will give insight in the completeness of the findings;
- validate the findings on the basis of significantly more interviews with experts, case studies and pilots;
- further research about the different CA & CM tools will highlight the extent to what these tools can be of added value for PM;

Contents

Preface

When I started to realize it was time for me to leave an exuberant and enjoyable university life behind, KPMG gave me the opportunity to do an interesting graduation project with them. After a few tests and meetings with recruiters and (future) colleagues, I started my graduation project six months ago. The objective was to successfully perform a graduation research with both, theoretical and practical relevance, and with the result in front of me I believe I have succeeded.

Of course, apart from the quantifiable benefits, most of all I have learned a lot about Continuous Auditing (CA) & Continuous Monitoring (CM), and enterprise-wide risks and performance management. Looking back, I think that there are quite some comparisons between graduating, and doing an IT-audit at an external organization. Just like an IT-audit, knowledge is hidden somewhere in places that you have to discover and explore, and when you have found the knowledge you have to assess it before you can use, improve or recover it. Furthermore with an IT-audit, external IT-auditors often interview an interviewee to gather more knowledge about specific subjects like IT General Controls (ITGC). I also interviewed experts and employees of three organizations in the Netherlands, but in my case to gather knowledge which could contribute to the research.

Now at the end of the research it is time to thank a number of people, without whom I would not have managed to bring this period to a satisfying end. First of all I would like to thank Menno, my supervisor from KPMG. He provided me with the necessary expertise at the right time, and challenging me to find solutions on my own. Second, to my supervisors at the University of Twente, Ton and Pascal. I would like to thank them for their opinions, comments and support during this period.

Furthermore, I would like to thank the organizations and individuals who contributed to the practical part of my research. Special thanks goes out to my colleague students, Marije, Jeroen and Vincent, for their many useful comments and all the help they provided during this thesis. Finally, last but not least, I would like to specially thank the people in my private environment. Many thanks to you all, as I could not have enjoyed and succeeded as much as I did without you.

I hope you will enjoy reading and be able to maximally profit from the content of this research. If you have any questions or comments, please do not hesitate to contact me. I will be happy to help.

Kind regards,

Koen klein Tank
Arnhem, February 18, 2011

Part I
Introduction

This part describes the context of the research and introduces the topic, problem statement and objectives. Furthermore, it provides the reader with some background information about the topic and in the end it presents the remainder of this thesis.

Contents of Part I

1 Organization

This section explains the organizational context of this research to enable readers to put the scope of the research into perspective. First, we give a high-level overview of KPMG and its activities. The second paragraph describes where the scope of our research (the added value of Continuous Auditing (CA) & Continuous Monitoring (CM) tools for Performance Management (PM)) fits into that bigger picture.

1.1 KPMG

KPMG firms are some of the world's leading providers of audit, tax, and advisory services. They now operate in 146 countries and have 140.000 people in all member firms around the world with more than 7.900 partners [KPMG International Cooperative, 2010]. KPMG provides audit, tax and advisory services to help organizations negotiate risks and perform in the dynamic and challenging environments in which they do business:

- Audit - Audit is an independent service that enhances the reliability of information used by investors and other stakeholders.
- Tax - KPMG's tax services are designed to help clients to achieve effective tax compliance, manage tax risks and control their associated costs.
- Advisory - Advisory works with clients to tackle challenges in transactions and restructuring, performance and technology and risk and compliance.

1.2 Advisory

This research will be conducted for the Advisory department of KPMG which works with clients to tackle challenges in Performance & Technology (P&T) and Risk & Compliance (R&C). KPMG's advisory practices combine specialist skills to provide objective advice and execution to help preserve and improve value. A business unit of Advisory is IT-Advisory (ITA).

IT Advisory assist organizations to identify and manage business technology risks. ITA professionals offer a range of services aligned to an organization's business IT life cycle to provide focused, client specific advice across all levels of the IT spectrum. Within ITA there are several practices. This research will be conducted for the practice R&C, in which KPMG professionals help organizations stay on track and deal with risks that could unhinge their business survival. For example, they are experienced in managing diverse issues including: fraud, regulatory compliance, risk frameworks and modeling, capital efficiency, corporate governance, dispute resolution, deriving value from contracts and many more [KPMG International Cooperative, 2010].

2 Research Approach

2.1 Background

Royal Ahold [Koninklijke Ahold, N.V., 2010] was one of the major success stories in the 1990s and is one of the major failures, suffering a complete meltdown, in 2003. The Ahold scandal became public in February 2003, when the organization announced that a series of accounting irregularities had overstated more than $880 million in profit booked in the previous two years. Subsequent disclosures revealed that Ahold's publicly reported earnings overall had been overstated by more than $1 billion.

In its initial announcement, Ahold said U.S. Foodservice, which supplies food to restaurants and hotels, had overstated income by inappropriately accounting for discounts from suppliers. According to Ahold, management at the unit booked more money in promotional allowances, which are provided by suppliers to promote their goods, than it actually received [de Jong et al., 2005].

This initial news in 2003 in combination with other scandals like Enron, WorldCom and Tyco has left the investor wary and lacking faith in the integrity of published financial reports [Flowerday and von Solms, 2005]. Confidence and trust needs to be reinstalled in the management and in the auditors [Flowerday and von Solms, 2005]. To restore trust is not an easy task, seeing that risk and trust appear to be contradictory variables. Shaw emphasized the need to manage risks, he stated:

> *"One may not manage risks, but one can manage for risks"* [Shaw, 2003].

This need accentuates the importance of an organization's Enterprise-wide Risk Management (ERM) to mitigate risks, and help ensure the accuracy of the information in their financial reports. In response to the numerous corporate failures arising from corporate mismanagement and fraud, new legislations are created such as the Sarbanes-Oxley (SOX) act of 2002 [Vasarhelyi et al., 2008].

SOX addresses many areas that affect the accuracy and transparency of financial reporting [Vasarhelyi et al., 2008]. The most important proposition in this legislation is the certification of financial statements which can be summarized as: CEOs and CFOs are required to personally sign and certify the correctness of financial reports [Datar and Alles, 2006]. Non-compliance with the SOX act results in significant penalties for CEOs and CFOs, including monetary fines and/or imprisonment [Datar and Alles, 2006].

This regulation and others like SAS70 and Basel II [Broady and Roland, 2008] have triggered the accounting professionals to reconsider what an audit means and how it is carried out. Several auditors proposed taking advantage of modern technology to bring auditing up to date to match the complexity of today's technology enabled global organizations [Alles et al., 2006b]. As Coderre states: "in today's regulatory environment, Chief Audit Executives (CAEs) are finding that their departments are becoming more and more consumed with the monitoring and testing of controls to meet demands of compliance" [Coderre,

2008]. This increasing amount of monitoring and testing drives the organization's costs to meet regulatory compliance. For example, in the United States, Jagan et al., pegged the cost of SOX compliance at an average of more than $2.2 million per organization [Jagan et al., 2008].

It is evident that new approaches, ones that provide a sustainable, productive, and cost-efficient means to address these issues are essential. Continuous Auditing (CA) & Continuous Monitoring (CM) are such new approaches. While the definitions of CA & CM may vary across organizations and industries, the purpose of these disciplines is to provide greater transparency, effectively manage risk, and provide continuous assurance [KPMG, 2009].

Although the continuous concept is over a decade old, the rapid advancements in technology has now made it feasible to update the traditional audit and monitor approach to the CA & CM approach [Flowerday and von Solms, 2005, CICA/AICPA, 1999]. Traditionally, financial reports where only produced on a periodic basis often months after the occurrence of the actual events they represent [Rezaee et al., 2002]. Auditing in this setting is mostly a backward-looking exercise (snapshot, [Kuhn and Sutton, 2006]) testing the accuracy of the reported numbers. Furthermore, it is often too late to be of real value for business performance or regulatory compliance [Coderre, 2008].

This in combination with corporate scandals (i.e., Ahold, WorldCom, Enron, and Tyco) has increased the demand for stronger corporate governance, risk management, improved internal-control and more transparent corporate reporting [Datar and Alles, 2006, Alles et al., 2006b, Kuhn and Sutton, 2006]. CA & CM and RM have received substantially greater attention as it is being viewed by auditors and management as approaches to fulfill this demand [Kuhn and Sutton, 2006].

These approaches will (continuously) monitor and manage an organization's transactions, comparing their generic characteristics to expected benchmarks, with this identifying unexpected situations [Alles et al., 2006b]. When unexpected situations occur, alarms are triggered and are routed to the responsible stakeholders. By using these techniques, organizations will improve the ability to mitigate fraud. The research of Kuhn and Sutton underpins this. According to them such approaches should have helped to detect the fraud of WorldCom [Kuhn and Sutton, 2006].

The focus of RM and CA & CM is not simply on compliance with controls and regulations, but also on the improved efficiency of operations in the organization. These approaches should contribute to the overall improvement of the organization by identifying and assessing risk and providing information to management in order to better respond to changing business conditions [Coderre, 2008]. In addition, objectives of the generally accepted framework for Enterprise Risk Management (ERM), the COSO ERM - Integrated Framework [COSO, 2004] already encourage management and auditors to approach their activities from a business perspective [Broady and Roland, 2008]. These objectives shift the focus of Risk Management (RM) from compliance with controls and regulations to improved efficiency of operations in the organization.

2.2 Problem Description

While the benefits of CA & CM are quite obvious, i.e., more comprehensive assurance with greater coverage across the organization [Coderre, 2008], organizations do not perceive it as a way to create value for their organization [de Schiffart, 2010]. The research of KPMG underpins this, a clear message out of their research is that according to managers the biggest benefits of CA & CM are believed to be in compliance and risk management [KPMG, 2010a]. According to the survey conducted by KPMG: one of the bottlenecks why managements are not creating plans for implementing such approaches [KPMG, 2010b]. This is a result of the perceived cost outweighing the perceived benefit. So the question is: How to make CA & CM interesting for the management of organizations?

To answer this question we must first know what is interesting for the management of organizations. Lets start at the top of an organization where the management is operating. Any organization, whether public or private, has to live within financial constraints and deliver perceived value for money to its stakeholders. It is the role of the management of organizations to keep the organization on the financial "straight and narrow" by performing as effective and efficient as possible [Otley, 1999]. Thus, anything that can possibly contribute to the performance of the organization will get attention from the management [Neely, 1999, Venkatraman and Ramanujam, 1986, Lebas, 1995, Lebas and Euske, 2002, de Schiffart, 2010]. As Venkatraman and Ramanujam state: "performance improvement is at the heart of management" [Venkatraman and Ramanujam, 1986].

Measuring the performance of an organization can briefly be described as evaluating the level to which organizational objectives have been attained [Neely, 1999]. Generally, profitability is used to evaluate organizational performance, but a single measure of performance cannot provide a clear concentration on the critical mission of organizations, as we will describe in Section 5 [Kaplan and Norton, 1996a]. Therefore, Performance Management (PM) tools are used to ensure that objectives are consistently being met in an effective and efficient manner, according to the mission and strategy of the organizations [Neyran and Nizamettin, 2007].

Problem Statement Based on literature [Cook et al., 1995, Kothari and Fesenmaier, 2006, KPMG, 2010b], we assume that if CA & CM to some extent can contribute to PM, it becomes more interesting for the management of organizations to implement such tools. For example, when organizations can use CA & CM to get a more comprehensive assurance with greater coverage across the organization, AND to enhance the quality and/or reliability of performance information, they may perceive CA & CM as a profit driver. However, nowadays the management of organizations does not, because they do not know to what extent CA & CM tools can be of added value for PM.

2.3 Research Objective and Questions

Based on the problems found and the literature available, the main objective of this research is:

> *Show the added value of Continuous Auditing (CA) & Continuous Monitoring (CM) for Performance Management (PM).*

The problems found in combination with the main objective of the research lead to the following research question:

> *To what extent can Continuous Auditing (CA) & Continuous Monitoring (CM) be of added value for Performance Management (PM)?*

To solve the main research question several sub-questions will be answered:

1. What is Continuous Auditing (CA) & Continuous Monitoring (CM)?
2. What is Risk Management (RM)?
3. What is Performance Management (PM)?
4. To what extent is there a relation between Continuous Auditing (CA) & Continuous Monitoring (CM) and Risk Management (RM)?
5. To what extent is there a relation between Risk Management (RM) and Performance Management (PM)?
6. To what extent can these relation be of added value for Performance Management (PM)?

After these questions are answered, interviews will be carried out at three organizations in the Netherlands and with three experts of KPMG. We will answer the following questions from a practical perspective by using the information gathered during these interviews:

7. What is the current situation of CA & CM, RM and PM tooling in these organizations?
8. To what extent are Continuous Auditing (CA) & Continuous Monitoring (CM), Risk Management (RM), and Performance Management (PM) related in organizations?
9. To what extent are Continuous Auditing (CA) & Continuous Monitoring (CM) and Risk Management (RM) adding value to Performance Management (PM) in organizations?

And finally, after we have gathered the theoretical and practical findings, we can compare them by answering the following question:

10. What can be concluded when comparing the findings from literature with the findings from practice?

2.4 Research Methodology and Structure

Figure 2 shows the structure of the research, divided in six main parts, depicted at the bottom of the figure. The structure is designed according to the techniques described by Verschuren and Doorewaard [Verschuren and Doorewaard, 2005]. The corresponding section numbers or appendix characters are shown in the top right corner of the blocks. The blue blocks present the theoretical part, the red blocks present the practical part, and the orange blocks present the synthesis of those parts. Finally, the green blocks represent the conclusions and further research. The structure is iterative as depicted with gray vectors below the blocks.

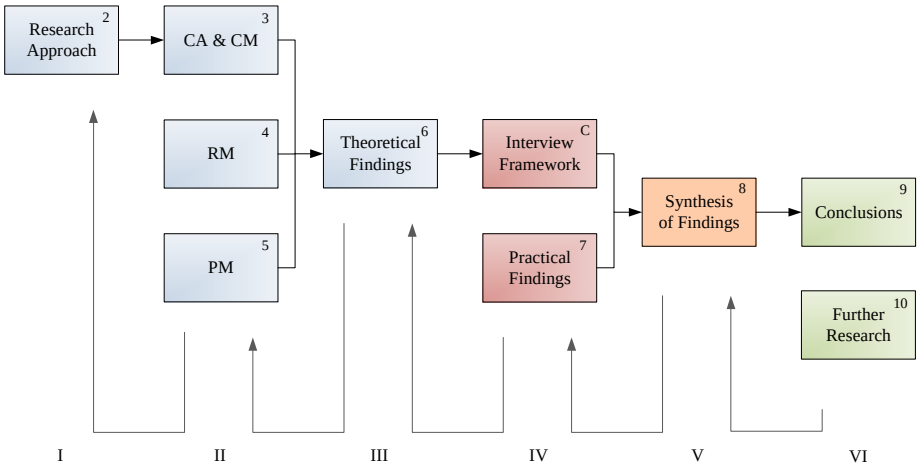

Figure 2: Research Structure, from [Verschuren and Doorewaard, 2005].

The first part consists of an extensive orientation on the research topic. Literature is consulted to get insight into CA & CM, RM and PM, and the problems arise in these research areas. All the activities in this part deliver a first impression of the problems, objectives, research questions and approach to solve those questions.

Part II provides the reader with the theoretical background about the research topic. In this part, an in depth literature review will be performed in order to get a detailed description of CA & CM, RM and PM.

The third part aims at combining the findings from Part II with new insights out of literature, to be able to create a first impression about the extent to what CA & CM can be of added value for PM.

In Part IV interviews will be carried out with employees of three organizations in the Netherlands to get practical insight into the current situation of CA & CM, RM and PM and how they are related and adding value. Furthermore interviews will be conducted with three employees of KPMG: experts on the CA & CM, RM and PM area. In addition, we visited two seminars about CA & CM. These interviews and the information gathered during the seminars will

contribute to the research and will provide insight and information completeness to achieve the objectives described in Sub-Section 2.3.

The information derived from these interviews will be compared with the first impression gathered out of literature. De results of this synthesis are presented in Part V.

In Part VI the final conclusions and recommendations will be drawn. In addition to that, some further research is presented. After this phase, the results could be exposed to KPMG and their customers who are interested in CA & CM. Furthermore the final thesis will be finished and presented to the graduation committee.

2.5 Impact and Relevance

This research will provide information about the extent to what organizations can add value to PM by implementing CA & CM. By doing so it contributes in a practical and theoretical perspective to different parties. The following two paragraphs describe the impact and relevance of this research from respectively a practical and a theoretical perspective.

Practical Relevance The practical relevance of the research for KPMG is: if KPMG is capable of convincing the management of organizations about the advantages of CA & CM in relation with PM, we assume that organizations are less reluctant to update their manual checks to automated checks by implementing CA & CM tooling.

So at best, the result of the research should be a motivation for the management and auditors to implement such monitoring activities. Not only to satisfy the demands for assurance, but also as a way to add value to the PM of their organization.

Theoretical Relevance From the scientific point of view, the research contributes to the theory development of CA & CM, RM and PM. Much has been published in these areas. Although these studies are insightful, they do not address the need for a research which describes to what extent CA & CM can be of added value for PM.

For example there is literature available which has been published on the benefits and implications of CA & CM [Searcy et al., 2003, KPMG, 2010a, Kogan et al., 2010, Alles et al., 2008]. Alles et al., wrote a paper where they reviewed the lessons learned over the last 20 years of attempting to move CA & CM from concept to practice [Alles et al., 2008].

Also a lot of authors have conducted their research on the implementation of CA & CM. Coderre and Rezaee et al., published reports which provides guidance for auditors and management on how to implement an ideal strategy combining CM & CA solutions [Rezaee et al., 2002, Coderre, 2008]. Furthermore, Alles et al., created a report about the approach they have developed and the lessons they have learned in an implementation of the monitoring and control layer

for CA of business process controls in the US internal IT audit department of Siemens Corporation [Alles et al., 2006a].

In the performance area, Forsythe wrote a book about managing performance in the American government. He examines the problems and possibilities of different PM tools and its role in government at the local, state, and federal levels [Forsythe, 2001]. PM should help organizations align their daily activities with their strategic objectives [Parmenter, 2010]. The book of Parmenter can help with this [Parmenter, 2010]. The book has been written to assist management in developing, implementing, and using Key Performance Indicators (KPIs). The ones he describes as those performance measures that will make a profound difference [Parmenter, 2010].

When searching for literature which combines risks and performance, we found some articles which elaborates on the combination of PM and RRM [Beasley et al., 2006, Ernst & Young, 2009, Broady and Roland, 2008]. For example the article of Ernst & Young in which a comprehensive risk and management approach is developed that takes into account strategic, operational, financial and compliance risks [Ernst & Young, 2009]. The article of Beasley is even more detailed and is focused on a combination of the Balanced ScoreCard (a PM method) and Enterprise-wide RM as the title explains: "Working Hand in Hand: Balanced Scorecards and Enterprise Risk Management" [Beasley et al., 2006].

2.6 Research Outline

In this section, the problems, research objectives, approach, and some background information about the research topics are presented. Sections 3, 4, and 5 of Part II provide the reader with the theoretical background about CA & CM, RM and PM. Then in Section 6, the relations between those will be illustrated. Furthermore, this section elaborates on how these relations add value to PM. Section 6 is the last section of the theoretical study.

Part IV provides the reader with information about the current situation of CA & CM, RM and PM, how they are related, and how they add value to PM at three organizations in the Netherlands. As additional information, this part describes the experts' view gained from interviews with three experts of KPMG.

Part V links the theoretical findings of Part III with the practical findings from Part IV. This will result in the conclusions and some recommendations in Part VI. In addition, we present some possibilities for further research.

Part II
Theoretical Background

This part establishes the theoretical background for the remainder of the research. With this part we try to create an understanding about the concepts of CA & CM in Section 3, RM in Section 4, and PM in Section 5.

Contents of Part II

3 Continuous Auditing (CA) & Continuous Monitoring (CM)

There are certainly similarities between CA & CM, but they are not quite the same. Understanding CA & CM, their relation, and how they differ is important. The next sub-sections elaborate on these topics.

3.1 Continuous Auditing (CA)

Traditionally, testing of controls has been performed by auditors on a retrospective and cyclical basis (e.g., ones a year, in regards with the annual audit), often many months after the business activities have occurred [Ibrahim and Hallemeesch, 2008]. Nowadays, technology has a major impact on the audit process. For example, computers are used to generate client specific internal control templates to help identify strengths and weaknesses in a system [Bierstaker et al., 2001].

However the use of such technology, auditing in this setting is mostly a backward looking exercise (snapshot, [Kuhn and Sutton, 2006]), testing the accuracy of the reported numbers. Often too late to be of real value to business performance or regulatory compliance [Coderre, 2008, Li et al., 2007]. Furthermore, the majority of the costs (average $2.2 million for SOX compliance per organizations in the United States) are related to manual, people intensive processes, based on internal resources and external consultants (e.g., external auditors of KPMG) [Jagan et al., 2008]. For these reasons, the focus of the audit shifts from manual detection to technology-based prevention as depicted in Figure 3 [Bierstaker et al., 2001].

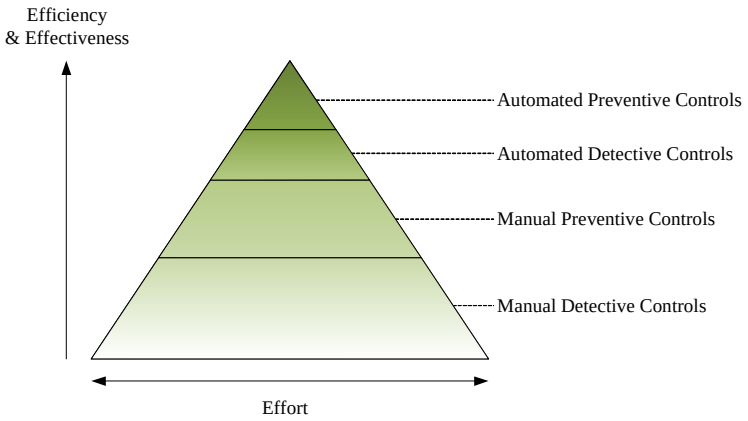

Figure 3: Control hierarchy, from manual detection to automated prevention, from [Bierstaker et al., 2001].

This figure illustrates the reduced effort and increased efficiency of automated controls. It shows that automated internal controls are like speed cam-

eras: they catch every single violation of a control instead of the occasional scofflaw. And like speed cameras, they reduce effort: after you install speed cameras on a highway or residential street, police officers do not have to sit around with radar guns looking for vehicles going over the speed limit, pulling them over, and writing tickets.

Continuous Auditing (CA) can be used to perform testing of controls and risk assessments automatically on a (more) frequent basis using intelligent software tools [Flowerday and von Solms, 2005]. The most widely accepted definition though, is one described in the CICA/AICPA research report of 1999:

> *"CA is a methodology that enables independent auditors to provide a written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter"* [CICA/AICPA, 1999].

This concept is not new. CA has been explored by auditors since the 1980s [Heffes, 2006]. Early adopters within the audit profession began using Computer-Assisted Audit Tools (CAAT) and techniques for investigation and analyses. In the 1990s, within the global audit profession, data analytics solutions were viewed as a critical tool to support the testing of effectiveness of controls. This "electronizations" leads to paperless accounting systems [Bierstaker et al., 2001]. For example, Enterprise Resource Planning (ERP) access and authorization tables could be analyzed to identify failures and to maintain appropriate Segregation of Duties (SoD) [Coderre, 2008, Li et al., 2007, Flowerday et al., 2006]. However even with this technology, audit processes often relied on samples and snapshots rather than assessing the entire/complete population of business activities on a continuous basis [Kuhn and Sutton, 2006].

Nowadays, information systems in the business environment give auditors easier access to a more relevant and complete set of information which makes it easier to identify and respond to risk and control issues. As Coderre stated: "technology plays a key role in the CA process by automating the pattern analysis of key numeric fields and the examinations of trends. Technology also enables the comparison of detailed transaction analysis against specific thresholds, the identification of exceptions and anomalies, the testing of controls, and the comparisons of processes or systems over time" [Coderre, 2007]. In our opinion the CICA/AICPA group [CICA/AICPA, 1999] does not sufficiently emphasize on IT in their definition of CA. The definition of KPMG [KPMG, 2009] better accentuates the importance of IT and will be used in the remainder of this research:

> *"CA is the collection of audit evidence and indicators by an auditor on Information Technology (IT) systems, processes, transactions, and controls on a frequent or continuous basis throughout a period"* [KPMG, 2009].

We think this definition contains the most important characteristics of CA: It is providing *auditors* with *control indicators*; these *indicators* are collected

out of *IT system, process, control, and transaction data*; and the information is collected on a *continuous basis*. The indicators for CA & CM are often expressed as *Key Control Indicators (KCIs)* or Key Risk Indicators (KRIs) [Flowerday and von Solms, 2005, Nigrini and Johnson, 2008]. In this research we will use *KCIs* to express the indicators of CA & CM.

We will illustrate the benefits of CA by means of an example:

Example. *Organizations can use CA to help to ensure that the procure-to-pay cycle is being executed without fraud. CA enables the organization to assess whether the person who is doing the purchase, the person who is doing the goods receipt and the person who is doing the payments are different (SoD). When unexpected situations occur (e.g., one and the same person is doing goods receipt and payments), alarms/notifications are triggered and routed to the auditors. In this way the auditor will be noticed about the situation, shortly after the actual event occurred [Bierstaker et al., 2001].*

A key issue that impacts the internal auditor's effort to CA is the extent to which management has implemented systems to monitor controls continuously and identify/control deficiencies and indicators of control (KCIs).

3.2 Continuous Monitoring (CM)

Continuous Monitoring (CM) refers to the processes that management put in place to ensure that the policies, procedures, and business processes are operating effectively. It typically addresses management's responsibility to assess the adequacy and effectiveness of controls. As explained in the section about CA, many of the techniques management is using in CM are similar to those performed in CA by internal auditors [KPMG, 2009]. The IAA defines CM as:

> *"CM is a process to ensure that policies and processes are operating efficiently and to assess adequacy and effectiveness of controls"* [CICA/AICPA, 1999].

In our opinion, the main difference is that CM should be performed and owned by management, as part of its responsibility to implement and maintain effective control systems. Because management is responsible for controls, they should have a means to determine, on a continuous basis, whether the controls are operating as designed [CICA/AICPA, 1999]. The definition of IAA does not emphasize on the responsibility of the management, which in our opinion is a key difference between CA and CM. For this reasons we created a new one based on definitions from KPMG and Deloitte [KPMG, 2009, Deloitte Development LCC, 2010]. We will use this definition in the remainder of this research, because we think this one better accentuates on the key characteristics of CM.

> *"CM enables management to continually review indicators in processes to ensure that controls operate as designed and transactions are processed as prescribed by detecting associated risk issues".*

If the *management* is able to monitor indicators to *identify risk issues* that can affect *business* processes and *correct control problems* in a *short period of time* after the actual event, the overall control system can be improved [KPMG, 2010a]. We will illustrate the benefits of CM by means of an example:

Example. *Organizations can use CM to help align the components of the procure-to-pay cycle, so they do not pay vendors in advance of the terms allowed by the contract and then need to access a credit line to support the difference. CM enables the organization to evaluate the date of the purchase, the date of goods receipt, and the date of payment; to align its payments with those parameters and the contractual terms and conditions with the vendor [KPMG, 2010a].*

Despite the differences between CA and CM, many of the CM techniques used by management are similar to those performed by auditors during CA . In the next sub-section we will describe the relation between, and the overlap of these two techniques.

3.3 Relationship CA & CM

Neither CA, nor CM needs to be present for the other to be implemented. Some organizations have successfully implemented CA without a CM tool in place [KPMG, 2009]. However, there is an inverse relationship between the sufficiency of management's monitoring and risk management activities and the extent to which auditors must perform detailed testing of controls and assessments of risks. As Coderre stated in his report, "the audit's activity to, and amount of CA depends on the extent to which management has implemented CM" [Coderre, 2008]. In Figure 4 this relationship is depicted.

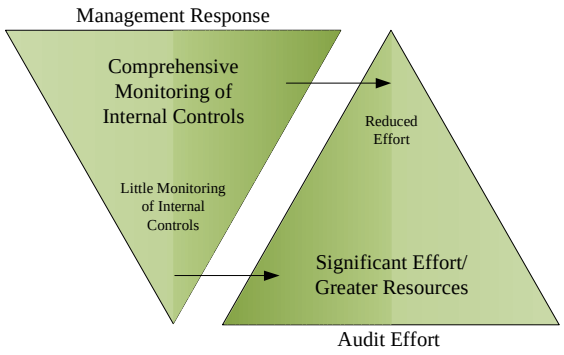

Figure 4: Relationship, level of effort expended by management and the audit activity, from [Coderre, 2008].

In Figure 4 you can see that in areas where management has not implemented CM, auditors should put much more effort by employing CA techniques. Where management performs CM on a comprehensive basis across end-to-end business process areas, the internal audit activity no longer needs to perform the same

detailed techniques that would otherwise be applied under CA. As Kemper stated:

> *"Reinventing the wheel would be a waste of time"* [Kemper, 2005].

A strong CM function can give management a vision into their operations, requiring auditors to focus on different aspects or combinations of the risks being monitored. In general, these procedures are similar to those quality control tests performed during the traditional audit process to ensure that CAAT have been applied correctly. If an organization does both, assessing the combined results of the CM with those of the CA, auditors are able to provide continuous assurance regarding specific transactions, business or governance processes, controls and systems as depicted in Figure 5.

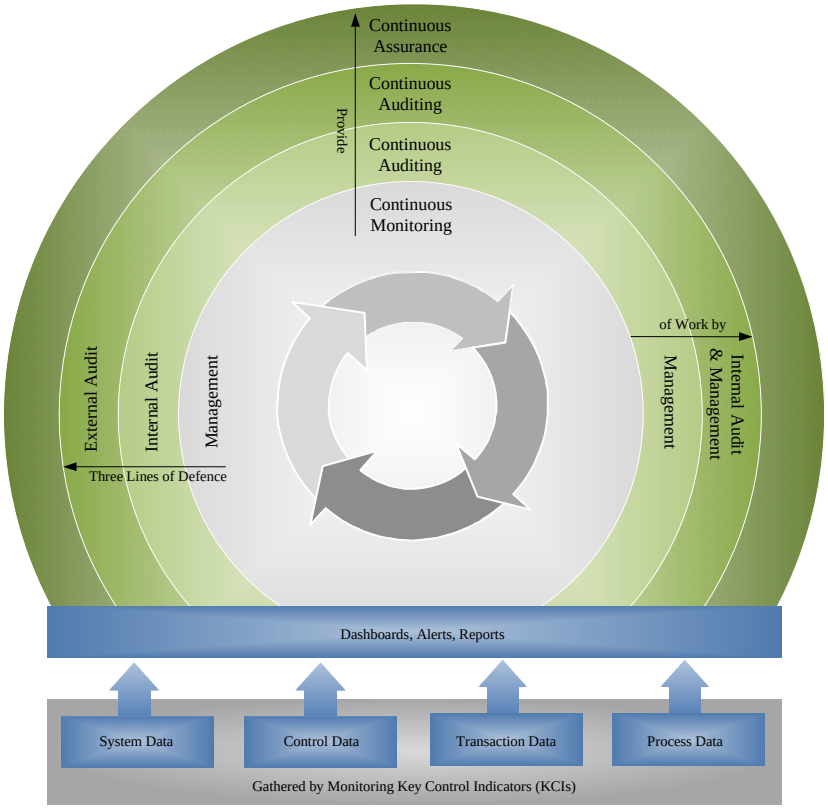

Figure 5: CA & CM model to provide continuous assurance.

The CA & CM model of Figure 5 integrates management's responsibility to monitor risk and internal control performance with how the internal and external auditors need to provide a risk-based level of assurance over management's controls and monitoring capabilities. This model demonstrates the three lines

of defense provided by the organization's governance structure, with each layer ensuring that it can rely on the work of the previous layer.

The data that is analyzed through dashboards, alerts and reports come from many sources and is gathered by monitoring KCIs. Some KCIs will be monitored manually, while others will be extracted automatically using tools such as SAP GRC, Oracle GRC, Approva, ACL, BWise, Xactions, and SynAxion. These tools are briefly described in Appendix A. Organizations that have a higher proportion of automated controls and data feeds that provide objective measurement of risks should benefit from this approach and from the efficiencies available as we will describe in Part III.

The continuous aspect is more than only monitoring on a higher frequency. In many literature, the completeness of data analysis is not mentioned as a key characteristic. We think CA & CM is both, monitoring at a higher frequency (not real-time as described in many literature, [KPMG, 2010a, Flowerday et al., 2006, Deloitte Development LCC, 2010]) and monitoring the complete data set. Furthermore we see a lot of different terms used for the indicators which are monitored. Examples are: KCIs, KRIs, and KPIs. In this research we express the indicators of CA & CM as Key Control Indicators (KCIs).

Often, this continuous assurance is considered to be strictly an audit-related activity, usually financial in nature. However, others, such as those in the legal profession, provide assurance services as well. Audit assurance is a statement regarding the adequacy and effectiveness of controls and the integrity of information. The continuous monitoring of controls is as depicted in Figure 5 at the core of effective assurance strategies. However, the audit activity must ensure that management activities are adequate and effective. Auditors examine the activities performed by management, verify that controls are working, recommend changes, and ensure that risks are being managed. If auditors do their job, then the organization will have a higher level of assurance that controls are working, risk are being managed, and the information used for decision making has integrity, while the management plays a role in assurance equation by developing, designing, and monitoring controls [Bierstaker et al., 2001].

3.4 Concluding

In this section CA & CM are discussed and some examples are presented. Based on this discussion we can define a set of key characteristics. The list of characteristics is established based on a comparison between the different theories. We think that organizations should think about the following characteristics before they start implementing CA & CM:

- we think that CA & CM together can deliver greater value to an organization than when they are implemented independently of each other;
- CA should be performed by auditors, while CM activities should be performed by the management as illustrated in Figure 5;

- a minimum of 60 or 70 percent of controls should be automated (based on a seminar about the status of CA & CM in the Netherlands);
- the organizations that have standardized automated processes are more likely to succeed in leveraging their investment in CA & CM across the entire organization;
- CA & CM activities should be centralized, thereby enabling that systems can be centrally monitored;
- indicators of CA & CM should be expressed as Key Control Indicators (KCIs).

In Part IV, we will describe the current situation of CA & CM in three Dutch organizations. This data is gathered from interviews with employees and experts on the field of CA & CM. The interview questions are described in Appendix C, Sub-Section C.4 and are based on the earlier derived characteristics as presented above.

Concluding, CA & CM is a valuable enabler and the number of providers (Appendix A) is expanding all of the time. Although it facilitates analysis of the complete set of data, allows high frequency monitoring of transactions and controls, and provides alerts for problems and anomalies, technology should not be the starting point to implementation, as we will see in the next part.

4 Risk Management (RM)

Risk is a fact of life. No matter what your plans are, whether it is crossing the street, going on vacations, play soccer, or buy a new product. Risk is inevitably involved [Broady and Roland, 2008]. However, not all risks are bad. Effective Risk Management (RM) can allow organizations to protect the value that they have build ("risk awareness" and "risk tolerance"), but it also allows organizations to create value by identifying opportunities, also described as "risk appetite" [Ernst & Young, 2010]. This section defines risk, describes Enterprise Risk Management (ERM) and discusses how organizations can use ERM to both protect and create value. This section also elaborates on the COSO ERM - Integrated Framework, which is the most used framework for RM [COSO, 2004].

4.1 Risk

Risk is typically defined as:

> *"The potential for loss caused by an event that can adversely affect the achievement of an organization's objectives"* [Harland et al., 2003].

Or as:

> *"a chance of danger, damage, loss, injury or any other undesired consequences"* [Harland et al., 2003].

Although these definition are true, it is only part of the story. According to Broady & Roland, risk awareness can also inform strategy, helping organizations select the opportunities to pursue that are most likely to succeed and that offer the most bang for the buck [Broady and Roland, 2008]. That is why we say that risk can both help organizations protect their value (protect what they have got) and create value (help organizations figure out the best way for their business to go in the future). As Ernst and Young state: "designing an organization's risk management without defining their risk appetite is like designing a bridge without knowing which river it needs to span. Your bridge will be too long or too short, too high or too low, and certainly not the best solution to cross the river in question" [Ernst & Young, 2010]. Risk appetite is typically defined as:

> *"the amount and type of risk an organization is willing to accept in pursuit of its business objectives"* [Ernst & Young, 2010].

As we will see later in this section, defining risk appetite is very much a task for the management, as it is intimately linked to defining the overall objectives of an organization. Risk appetite regarding the organization's strategic objectives should first be translated into 'risk tolerance'. Risk tolerance can be expressed as:

"the specific maximum risk that an organization is willing to take regarding each relevant risk" [Ernst & Young, 2010].

Risk tolerance can be set for specific categories of risk. Out of the researches of Harland et al., and Drew, we can divide risk into four different categories as depicted in Figure 6 [Harland et al., 2003, Drew, 2007].

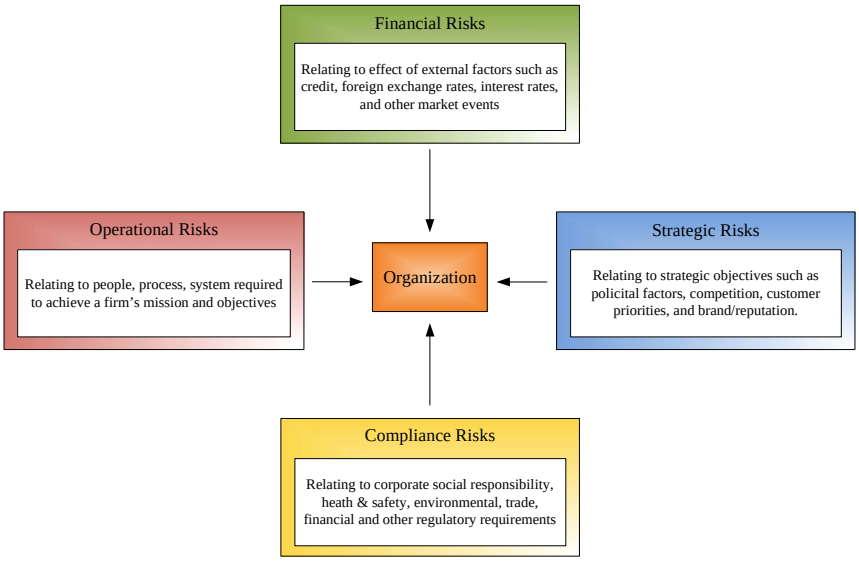

Figure 6: Four categories of business risks

Although some of the risks in these categories might be considered negative, keep in mind that some risks can also result from success. Examples are: a product launch where demand is much greater than anticipated; a founder may be a great entrepreneur and company starter, but not have the skills to keep the company growing at that initial pace. Just as both positive and negative events produce stress in our lives. For example, weddings and new babies are positive events, but undeniably stressful. So business success can bring stress and associated risks as well. The risks of success should also be taken into account in order to protect value in the present and create value in the future.

You have likely heard the saying, "no risk, no return". We think taking risks is part of being a successful organization. Rather than not taking risks, systematically cataloging, evaluating an managing core risks, as we discuss in this section, can be thought of as helping organizations to take the right risks, the ones most likely to pay off. Furthermore, rather than running around and gathering information about all the risks of the organization, technology (e.g., CA & CM tools) can help by monitoring and reporting the risks organizations want to manage.

4.2 Enterprise Risk Management (ERM)

Although some organizations have employed sophisticated RM processes, others take a firefighting or ad hoc approach to RM. With such approach, RM is mainly intuitive. Much of the knowledge of an organization's risks is kept in someone's head. But in the aftermath of the financial crisis, executives and their boards realize that this ad hoc RM approach is no longer tolerable in today's rapidly evolving environment. Increasingly, boards and management teams are embracing the concept of Enterprise Risk Management (ERM) to better connect their risk oversight with the creation and protection of the organization's value.

ERM differs from the more traditional RM approach, frequently described as "the silo or stovepipe approach, where risks are often managed in isolation" [Beasley et al., 2006]. It includes the methods and processes used by organizations to manage risks related to the achievement of their objectives [COSO, 2004]. Thereby, helping organizations ensure that it designs efficient and effective controls and activities to mitigate a range of strategic, operational, financial, and compliance risks [Ernst & Young, 2010]. Such a program defines accountabilities as well as what Key Risk Indicators (KRIs) to monitor, how to monitor, and at what frequency to monitor [KPMG, 2009]. From our point of view, the ultimate goal of ERM is to ensure that the value of the organization is preserved and/or even enhanced. The Committee of Sponsoring Organizations of Treadway Commission [COSO, 1994], which developed a conceptual framework for Internal Control and ERM, defines ERM as follows:

> *"Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"* [COSO, 2004].

We will use this definition in the remainder of this research, because we think it contains the key characteristics of ERM. ERM is effected by *all employees* of an organization, applied in a *strategy setting* across the *enterprise*. Manage risk within its *risk appetite*, and provide *assurance* regarding the achievement of *entity objectives*.

In Section 3, we discussed CA & CM and how these approaches can provide compliance with laws and regulations. By complying with these laws and regulations (e.g., SOX), organizations avoid fines and ensure that their business processes and policies are effectively implemented. In a sense, compliance is nonnegotiable, organizations have to make sure that they do the things that they have to in order to comply with laws and regulations that govern their business [Broady and Roland, 2008].

ERM is more strategic and its potential impact is greater as well. With an effective ERM, organizations can both help protect value (e.g., brand name, quarterly earnings, and sales) and create value, evaluating the impact of strat-

egy, operational, financial and compliance risks on strategy execution as well as finding new opportunities and evaluating them from a risk perspective.

Organizations performing ERM often have build their risk management approach based on COSO's ERM - Integrated Framework [COSO, 2004]. In the early 1990s, COSO published the Internal Control - Integrated Framework to help "businesses and other entities assess and enhance their internal control systems" [COSO, 1994]. This became necessary or sometimes inevitably for organizations, because section 404 of the SOX regulation requires organizations build up an internal control system that is checked by the organization itself (e.g., CEO, CFO or internal auditor) and by an external auditor (e.g., KPMG) [Broady and Roland, 2008].

During the 1990s, the need for improved ERM was identified as a major concern across industries and governments. Reacting to this need, COSO initiated a project in 2001 to develop a framework that would help management to improve their organization's RM [Bowling and Rieger, 2005]. The resulting framework expanded on the existing Internal Control - Integrated Framework [COSO, 1994], aiming to provide "a more robust and extensive focus on the broader subject of risks management" [COSO, 2004]. In the next sub-section we will elaborate on the framework to create a better understanding of enterprise-wide RM and the activities it includes. Furthermore this framework will be used to create understanding about the link between CA & CM and ERM in Part III.

4.3 The COSO ERM - Integrated Framework

COSO's ERM - Integrated Framework encourages auditors to approach their ERM activities from the way management runs a business: control environment, risk assessment, information and communication, and risk monitoring. The framework is illustrated in Figure 7.

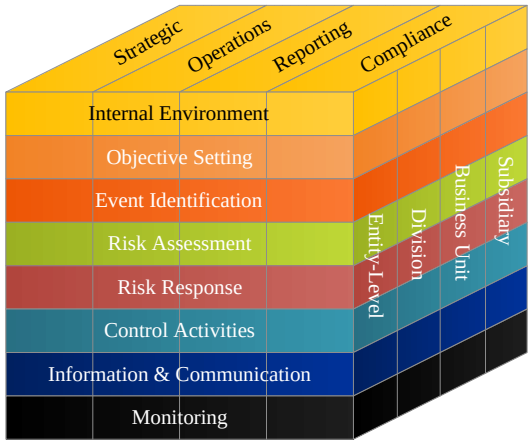

Figure 7: The COSO ERM - Integrated Framework, from [COSO, 2004].

Figure 7 depicts the relationship between objectives, which are what an entity strives to achieve, and ERM components, which represent what is needed to achieve them.

Looking at the mission and vision of an organization, management establishes strategic objectives, selects strategy, and sets aligned objectives throughout the organization. The COSO ERM - Integrated Framework is geared to help to achieve an organization's objectives, set forth in four categories at the top of the cube: strategic (high level objectives), operations (effective and efficient use of its resources), reporting (reliability of reporting), and compliance (compliance with laws and regulations).

These four categories put pressure on auditors to evaluate the internal control and to identify and assess risks to contribute to the achievement of the objectives [Coderre, 2008]. To do this, auditors must change their role to one that focuses on corporate objectives, strategies and RM, as well as critical control activities [COSO, 2004].

The eight horizontal rows consist of eight interrelated components:

Internal Environment The organization's environment is the foundation for all other components of ERM, providing discipline, governance and structure. The internal environment comprises, e.g., ethical values, managements operating style and how it assigns authority and responsibility.

Objective Setting For an organization's mission or vision, management establishes strategic objectives, selects strategy, and establishes operational reporting and compliance objectives at different levels of the organization, aligned with and linked to the strategy.

Event Identification Management recognizes that uncertainties exist: it cannot know with certainty whether and when an event will occur, or its outcome should it occur. As part of event identification, management considers external and internal factors, e.g., economic environment, technological factors, and personnel, that affect event occurrence.

Risk Assessment During risk assessments, potential events are analyzed to investigate their influence on the achievement of objectives. Management assesses events from two perspectives: likelihood, the possibility that a given event will occur, and impact, the effect of an event, should it occur [Drew, 2007].

Risk Response Possible risk responses are identified and their effect on event likelihood and impact, in relation to risk tolerances and costs versus benefits, are considered.

Control Activities Control activities are the policies and procedures for executing risk responses properly. Control activities occur at all levels in an organization, and are part of the process by which an organization strives to

achieve its business objectives. Relying on complex information systems these days, introduces a necessity for internal controls. Two groups of controls are distinguished: application controls, built within applications, and IT General Controls (ITGC), which are controls over information technology management, e.g., security management and software acquisition.

Information and Communication External and internal information is identified, captured and communicated in a form and time frame that enable personnel to carry out their responsibilities. Effective communication also occurs in a broader sense, throughout the organization and to external parties. Information is needed at all levels of an organization to identify, assess and respond to risks.

Monitoring Controls set, can be monitored by assessing aligned risk indicators, in this research expressed as KRIs. KRIs are monitored, to address the functioning of an organization's ERM components (e.g., controls) and the quality of their performance over time. Monitoring is accomplished through ongoing management or auditing activities, separate evaluations, or both with e.g., manual activities, or automated activities like CA & CM.

According to COSO, these are derived from the way management runs an organization and are integrated with the management process. There is a direct relation between the objectives, which are what an entity strives to achieve, and the components, which represent what is needed to achieve them.

The third dimension of the cube outlines different levels of the organization. Most importantly, it starts with the broadest level, the entity (or entire organization) and proceeds to a subsidiary level. This portrays the ability to focus on the entirety of an organization's ERM, by objectives category, component, entity unit, or any other subset before [COSO, 1994].

4.4 Concluding

This section discusses RM and it briefly describes the COSO ERM - Integrated Framework. Based on this discussion we define a set of key characteristics. The list of characteristics is the result on a conformity between the different theories. In our opinion, organizations should think about, and take into account, the following characteristics before they start implementing a RM approach:

- risks is a fact of life and could destroy and create value of organizations, therefore organizations should be aware of risks, and define their risk appetite and tolerance;
- we distinguish four different categories of risk: strategic risks, operational risks, financial risks, and compliance risks;

- organizations should take a systematic approach to RM, for example by adopting a framework that leverages technology to collect, monitor, and manage the key risks;
- RM should be geared to help to achieve an organization's objectives and strategy;
- RM should be part of the culture of the organization and this support should start at the top with the executive board;
- KRIs should be aggregated throughout the organization, from top (strategic) to bottom (operational);
- RM should be an iterative and continuous process;
- if possible, the monitoring of risk indicators should be on a regulatory and automated basis;
- indicators of risk should be expressed as Key Risk Indicators (KRIs);
- not all risks can be monitored automatically, therefore manual monitoring activities will always be required.

Part IV describes the current situation of RM in three Dutch organizations. This data is gathered during the interviews with employees of the three organizations and during the interviews with experts of KPMG on the field of RM. The interview questions are described in Appendix C, Sub-Section C.4 and are based on the earlier derived characteristics as presented above.

5 Performance Management (PM)

As explained in Part I, it is important to understand why to measure organization's performance is both necessary and vital. Johnson accentuates the importance of performance measurement with some understandable examples: "an organization operating without performance measurement system is like an airplane flying without a compass, a Formula One race car driver guiding his car blindfolded, or a CEO operating without a strategic plan" [Johnson and Beiman, 2007].

Performance measurements is failing organizations all around the world, whether they are multinationals, governmental departments, or small local charities [Cook et al., 1995]. These measures are frequently monthly or quarterly. Management reviews them and says: "that was a good quarter" or "that was a bad month". They should help organizations align daily activities with strategic objectives [Neely, 1999, Lebas, 1995, Lebas and Euske, 2002]. Kothari and Fesenmaier state: "performance measures play a critical role in formulating corporate strategies, evaluating accomplishments, and compensating organizational members" [Kothari and Fesenmaier, 2006]. It are measurable characteristics, in this research expressed as Key Performance Indicators (KPIs), of products, services, processes, and operations the organization uses to track and improve performance.

> *"In order to improve something you have to be able to change it. In order to change it you have to be able to understand it. In order to understand it you have to be able to measure it"* [Kothari and Fesenmaier, 2006].

But measuring is complex, frustrating, difficult, challenging, important, abused and misused, yet, as Scott Sink once said:

> *"If you cannot measure, it does not exist"* [Sink, 2007].

A specific measure can be compared to itself over time, compared with a preset target, or evaluated along with other measures [Kothari and Fesenmaier, 2006]. But what is performance? how should it be measured and managed? And from which perspectives could be measured? In the remainder of this section these questions will be answered.

5.1 Performance

Simply, some people say: "performance is getting the job done". But this is not as simple as it sounds, people often mean very different things when they talk about performance. Yet, the term "performance" appears continuously in the management as well as engineering literature. According to Lebas, "few people agree on what performance really means. It can mean anything, from efficiency, to robustness or resistance, Return On Investment (ROI), or plenty of other definitions never fully specified" [Lebas, 1995, Lebas and Euske, 2002].

Using context to clarify the meaning may help to create a basis for understanding and discussion. In the research of Lebas and Euske, they have combined different terms of performance and out of that created a new one: "performance is the sum of all processes that will lead managers to taking appropriate actions in the present that will create a performing organization in the future (i.e., one that is effective en efficient)" [Lebas and Euske, 2002]. In other words, performance can be defined as:

> *"Doing today what will lead to measured value outcomes tomorrow"* [Lebas and Euske, 2002].

Performance is something each firm, each stakeholder, each organizational actor defines, measures, and manages [Lebas, 1995, Cook et al., 1995, Kothari and Fesenmaier, 2006]. As Broady & Roland state: "board of directors, Chief Executive Officers (CEOs), Chief Functional Officers (CFOs), another executives at all levels want an accurate view of the performance of their business" [Broady and Roland, 2008]. Performance is never objective, it is only a way of defining where one wants to go [Lebas, 1995].

5.2 Performance Measurement

While there are different meanings of the term "performance", there are even as much different definitions of the term "performance measurement" [Venkatraman and Ramanujam, 1986, Lebas and Euske, 2002, PwC, 2008, Davies, 1999]. Any article, book or paper you read on performance measurement will provide a working definition and each of these will say essentially the same thing. However, the term essentially is tricky. There are some different ideas about the measure part in the definitions. For example we think a good definition is:

> *"A performance measure measures something, usually progress towards an objective goal"* [Lichiello, 1999].

But there are also definitions which we see as a combination of performance measurement and management. Like the definition of Cook et al., [Cook et al., 1995]:

> *"The periodic measurement of progress toward explicit short- and long-run objectives and the reporting of the results to decision makers in an attempt to improve performance"* [Cook et al., 1995].

The last part of this definition: "the reporting of the results to decision makers in an attempt to improve performance", can be considered as a management activity. It is important to note that performance measurement itself has no consequence. Simply knowing that there is scope for improvement in an organization, because you have measured some aspect of its performance will not, in itself, lead to any improvement. So in order to get some improvement as a result of performance measurement, the organization needs to do something with this

information. The issues associated with: "doing something with performance measurement information", is in our vision covered by the more general topic of Performance Management (PM).

5.3 Performance Management (PM)

Again as with the terms "performance" and "performance measurement", different terms are used for "Performance Management" (PM) [Venkatraman and Ramanujam, 1986]. As PwC state in their article about corporate performance management: "not only is there no single definition of corporate performance management, there is also no single name for it" [PwC, 2008]. When they surveyed 112 senior executives of US-based multinational companies in late 2007 on the subject, 62 percent of the respondents said that improvement of corporate performance and reporting was one of their top corporate priorities. But when they were asked what they called their efforts in this area, respondents volunteered more than 40 names, including business performance management, performance management, corporate performance management, organization dashboard, enterprise information management, Key Performance Indicators (KPIs), and matrix management [Venkatraman and Ramanujam, 1986, PwC, 2008]. For the purpose of this research, we will use the term "Performance Management" (PM) which must be understood in the following terminology:

> *"Performance management is the use of performance measurement information to help set agreed-upon business performance objectives, allocate and prioritize resources, inform managers to either confirm or change current policy or program directions to meet those objectives, and report on the success in meeting those objectives"* [National Partnership for Reinventing Government, 1997].

In our opinion, this is a good definition because it accentuates on the use of performance measurement information, which distinguishes the difference between performance measurement and management.

With PM, managers can translate the organization's strategy into financial and operational plans and then measuring how well the organization is meeting those plans [Neely, 1999]. In the most advanced situation, these measurements are executed on a continuous basis. The result is an up-to-date view of how the organization is performing against its financial and operational goals and a powerful decision making tool for the management [PwC, 2008]. For example, a survey conducted by Lingle and Schiemann found that: "organizations which are tops in their industry, stellar financial performers and adept change leaders, distinguish themselves by the following characteristics: having agreed-upon measures that managers understand, balancing financial and non-financial measurement, linking strategic measures to operational ones, updating their strategic scorecard regularly, and clearly communicating measures and progress to all employees" [Lingle and Schieman, 1996].

5.4 Perspectives of PM

The challenge for organizations today is how to match and align performance measures with business strategy, structures and corporate culture, the type and number of measures to use, the balance between the metrics, the costs of introducing these measures, how to ensure the reliability of these measures, and how to deploy the measures so that the results are used and acted upon.

As long as business organizations have existed, the traditional method of performance measurement has been financial. Financial measurements are an essential part of the overall management process. At the turn of the twentieth century, financial measures were critical to the success of the early industrial giants, such as General Motors [Kothari and Fesenmaier, 2006, Niven, 2006]. According to Niven, this is not a surprise. He stated that: "since the financial metrics of the time were the perfect complement to the machinelike nature of the corporate entities and management philosophy of the day. Competition was ruled by scope and economies of scale with financial measures providing the yardstick of success" [Niven, 2006]. Typical of this approach could be to examine KPIs, as sales growth, profitability, and earnings per share. [Venkatraman and Ramanujam, 1986].

Financial measures of performance have evolved rapidly in the last decade with the development of new measurement approaches, frameworks and methodologies, such as Activity Based Costing (ABC) and Economic Value Added (EVA) [Kothari and Fesenmaier, 2006, Cooper and Kaplan, 1997]. These PM frameworks are described in Appendices B.1 and B.2.

While performance can be measured using financial PM methods, many professionals in the PM area are questioning about methods such as EVA and ABC [Niven, 2006, Kothari and Fesenmaier, 2006, Johnson and Beiman, 2007]. Therefore, over the past two decades, a great deal of attention has been paid to the development and use of operational (i.e., non-financial) measures of performance [Neely, 1999, Venkatraman and Ramanujam, 1986]. According to Venkatraman and Ramanujan, the inclusion of operational KPIs takes us beyond the black box approach that seems to characterize the exclusive use of financial KPIs and focuses on those key operational success factors that might lead to financial performance [Venkatraman and Ramanujam, 1986].

Such KPIs could be: market-share, customer satisfaction, new product introductions, product quality, marketing effectiveness, manufacturing value-added, and other measures of technological efficiency within the domain of business performance [Venkatraman and Ramanujam, 1986]. There are several approaches developed to move away from a concentration on accounting measures alone. For example: the Balanced ScoreCard (BSC), the Performance Prism (PP) and Quality Management (QM). These approaches are presented in Appendices B.3, B.4 and B.5.

5.5 The Integral Framework for Performance Measurement (IFPM)

There are many established frameworks available for PM as described in the previous sub-section. Next to these established frameworks, there are meta frameworks for PM as well. These frameworks do have a more theoretical view on PM, however though, they are an addition to the frameworks already discussed in the previous sub-section. In literature there are different meta-frameworks discussed, the most common are the ones of: Otley [Otley, 1999], Eccles [Eccles, 1991], Wisner and Fawcett [Wisner and Fawcett, 1991], and Rouse and Putterill [Rouse and Putterill, 2003]. This sub-section elaborates on the framework of Rouse and Putterill.

We will discuss this framework, because of its systematic approach to PM. The next section describes how RM and PM are related and can be integrated, and we think this framework can best be used to research the extent to what PM is related to RM. Rouse and Putterill have developed the Integrated Framework for Performance Measurement (IFPM), which attempts an integration of a number of structural frameworks and includes a set of principles that should be considered alongside the framework [Rouse and Putterill, 2003]. Figure 8 depicts the IFPM.

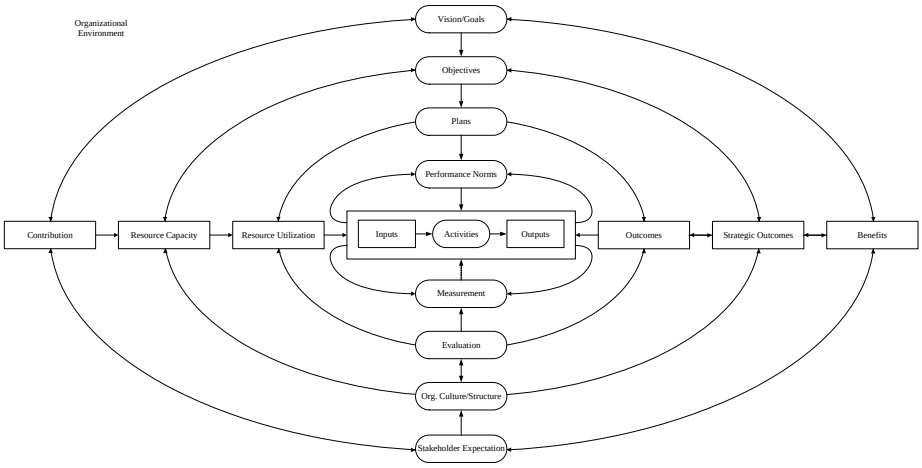

Figure 8: The IFPM, from [Rouse and Putterill, 2003].

Organizations can develop their PM according to the IFPM in four steps:

Step 1: the basic process core elements According to Rouse en Putterill, each process can be viewed as a collection of activities consuming inputs to produce outputs, as depicted in the middle square of Figure 8 [Rouse and Putterill, 2003]. The arrows from this square to "performance norms" and "measurement" introduces the basic notion of a control measuring process that compares activ-

ities against performance standards or norms. The outputs of these activities are inputs of the square, as the directional arrows in Figure 8 depict.

Step 2: planning-evaluation and resource-achievement dimensions In the second step (second circle from the inside) two views are depicted: the "resource achievement" (horizontal view) and the "planning evaluation" (vertical view).

In the vertical view "performance norms" are generated from, or in the course of "process planning", and "measurement" are depicted as essential prerequisite of the latter "evaluation process". This control loop can include both feed-back and feed-forward information flows for corrective actions as suggested by Otley [Otley, 1999].

In the horizontal view "resource utilization" and "outcome information" can be used to generate appraisal measures of effectiveness, efficiency and economy. Rouse and Putterill state: "moving from left to right, resource utilization when combined with input defines the conventional economic measures. The relationship between input and output measures efficiency, and effectiveness can be gauged by the relationship between outputs and outcomes" [Rouse and Putterill, 2003].

Step 3: organizational context The third step extends the previous step to incorporate an organization-wide context. This step is illustrated as outermost circle. The same as with enterprise-wide RM, managers should set the "objectives" of the organization which form the basis for plans that cascade down via "plans" to "performance norms". In order to achieve these "objectives", an organization must have appropriate "resource capacity" in place [Cooper and Kaplan, 1997].

The employees' link to "capacity" correspondents to the manner in which an organization is structured and the culture in place [Rouse and Putterill, 2003]. This structure and culture will also affect the "strategic outcomes". According to Rouse and Putterill, "strategic outcomes represent the official view and are a subset of the total outcomes shown in the previous step" [Rouse and Putterill, 2003].

Step 4: the overall framework This step represents the complete framework as illustrated in Figure 8. At the bottom, the "stakeholders" include owners, employees, partners, and the community. "Stakeholders" are represented at the outer circle, because they influence all levels of the organization. Their requirements and expectations define environment and general constraints that the organization must recognize in its operations [Rouse and Putterill, 2003].

An organization should define its strategy, goals, vision and mission based on the "stakeholders" expectations. "Contribution" deliver the resources used as inputs to production and service processes (material, labour and capital). On the other side of the framework, "benefits" reflect the value of the impact of the organization's "outputs" and "outcomes" (products, services) on "stakeholders"

expectations.

5.6 Concluding

In this section PM is discussed and some perspectives and methodologies are presented. Based on this discussion we can define a set of key characteristics of PM. The list of characteristics is derived out of a conformity between the different theories and the applicability on the different methodologies discusses in this section. In our opinion, organizations should think about, and take into account, the following characteristics before they start implementing PM:

- organizations should take a systematic approach to PM, e.g., by adopting a framework that leverages technology to collect, monitor, and manage the KPIs;
- KPIs should be aggregated throughout the organization, from top (strategic) to bottom (operational);
- PM should be an iterative and continuous process;
- the monitoring of KPIs should be on a regulatory and automated basis;
- the indicators which are monitored to manage an organization's performance should be expressed as Key Performance Indicators (KPIs);
- organizations should translate the organization's strategy into financial and non-financial indicators;
- PM should be supported by the top management, and they should clearly communicate measures and progress to all employees of the organization.

Part IV describes the current situation of PM in three Dutch organizations. This data is gathered during the interviews with employees of the three organizations and during the interviews with experts of KPMG on the field of PM. The interview questions are described in Appendix C, Sub-Section C.4 and are based on the earlier derived characteristics as presented above.

Part III
Theoretical Findings

This part provides the reader with information about how CA & CM, ERM and PM are related. It provides a model in which they keep performance and risks in balance. Furthermore this model creates understanding about how CA & CM can be of added value for PM. With this model the academic part of this research is concluded, enabling the next part to dive into practice.

Contents of Part III

6 Potential Added Value of CA & CM from a Theoretical Perspective

One thing is clear out of the literature research of Part II: most organizations' investment in CA & CM is a major one, so organizations must maximize the benefit from it [KPMG, 2010a, de Schiffart, 2010]. The fundamental idea is that CA & CM and PM should not be addressed in a narrow way, but in an integrated approach.

The theoretical study found out that there is a limited amount of literature available about the extent to what CA & CM is related with, or can be of added value for PM. But when diving deeper, we experienced that CA & CM and PM are often described in combination with Enterprise-wide RM (ERM) [Broady and Roland, 2008, KPMG, 2009, Beasley et al., 2006, Deloitte Development LCC, 2010, COSO, 2009, McKittrick, 2009]. Figure 9 depicts how CA & CM can be of added value for PM (directly, or indirect via ERM).

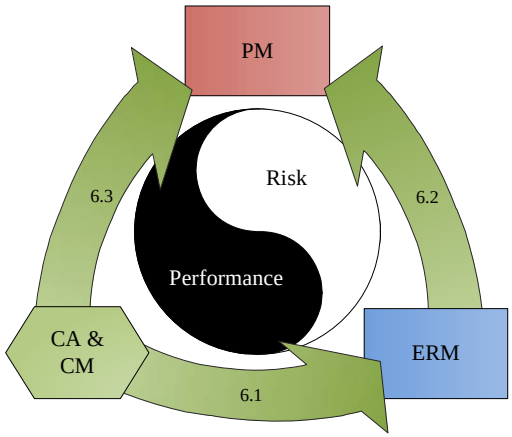

Figure 9: How CA & CM can add value to PM

We will start this section by creating understanding about the vectors from CA & CM to ERM in Sub-Section 6.1, ERM to PM in Sub-Section 6.2, and CA & CM to PM in Sub-Section 6.3. The outline of this section is depicted in Figure 9.

6.1 CA & CM and ERM

Because the objectives in the COSO ERM - Integrated Framework of Part II relating to reliability of reporting and compliance with laws and regulations are within the organization's internal control [COSO, 2004], CA & CM can be expected to provide reasonable assurance of achieving those objectives. However, we think the focus of CA & CM should not only be on the reliability of reporting and compliance with controls and regulations, but also contribute to

the achievement of the operational and strategic objectives.

The eight horizontal rows in the framework represent what is needed to build in ERM as an intrinsic component for all business processes [Bowling and Rieger, 2005]. Reading from top to bottom, the eight components start with internal environment and conclude with monitoring. Between them, there is a clear sequence of activities [Bowling and Rieger, 2005]. In other words, when an organization implements ERM for the first time, it needs first to understand its internal environment, before it sets objectives, identifies events, assesses risks and responds to those risks. As Ernst & Young state:

> *"You can only fix and improve what you have got if you have a very clear view of where to start"* [Ernst & Young, 2010].

The last three components in the sequence of eight are the most familiar, as they are components of COSO's Internal Control - Integrated Framework [COSO, 1994]: control activities, information and communication, and monitoring.

In fact when ERM is implemented, each component affects the others. As COSO state: "It is not strictly a serial process, where on component affects only the next. It is a multi-directional, iterative process in which almost any component can and does influence another" [COSO, 2004]. In this sub-section we will discuss the potential added value of CA & CM for PM on the basis of a literature study.

According to Deloitte, "often executives and boards consider ERM in broad terms, but have trouble bringing it down to the operational level" [Deloitte Development LCC, 2010]. Yet, at that level we think that CA & CM tools can be most beneficial for ERM and especially for the monitoring component of it [Broady and Roland, 2008, COSO, 2009].

Risks change over time and therefore there is a need for the management to "determine whether the internal control system continuous to be relevant and able to address new and existing risks" [COSO, 2009]. COSO recognizes effective monitoring of e.g., internal controls as a solution which can help to streamline the assessment process of ERM. Placed at the bottom of the horizontal components in the COSO ERM - Integrated Framework, the monitoring component is necessary to determine that all components of an installed ERM continue to work effectively [COSO, 2009, General Counsel Roundtable, 2003]. Coderre even states: "monitoring is the final COSO ERM component and is a key ingredient in an organization's effort towards continuous improvement" [Coderre, 2008]. This statement of Coderre accentuates the link between CA & CM, ERM and PM, as will be explained in the next sub-sections.

Monitoring often takes place by installing ongoing monitoring activities such as CA & CM, to be able to flag exceptions or violations of KRIs in some aspects of the overall ERM process [Broady and Roland, 2008, Davies, 1999, Moeller, 2007]. The outcomes of CA & CM involve notifications or alerts indicating deficiencies or potential risks. These notifications or alerts can be prioritized and,

depending on the seriousness of the risk or control deficiency, communicated to the stakeholders responsible for it [COSO, 2004]. CA & CM can contribute to ERM by helping to ensure the accuracy of information and the timely reporting of these alerts and notifications. We will explain this below.

The information ERM provides is much more valuable when it is timely. But nowadays, in many cases, information for both PM and ERM is collected through manual processes that create data that is stale, weeks or months behind the actual performance of the organization. Using such data is like attempting to drive a car by looking at the rear view mirror [Broady and Roland, 2008]. When using CA & CM, monitoring is not a hindsight process, but an ongoing concern and automating the process of e.g., testing controls is as "near" real time as possible. Management responsible for ERM can faster respond to risks, because they are earlier informed.

With CA & CM organizations can update the snapshot approach (e.g., taking a few records in the database) to an analysis about the complete set of information (all records in database). In this way, the accuracy of the reported information increases.

CA & CM can continuously analyze and assess risks, and define the likelihood and impact, so management can determine how, and which risks should be managed. The information (e.g., risks and opportunities) gathered from CA & CM activities can be channeled to the management for revising strategy and objectives, risks, and controls.

6.2 ERM and PM

In the previous sub-section we elaborated on the potential for CA & CM to add value to Enterprise-wide Risk Management (ERM). This sub-section provides the reader with information about the linkage between ERM and PM and how this can be of added value for PM.

In recent literature ERM is often described in combination with PM because of their similarities [Broady and Roland, 2008, Beasley et al., 2006, Cokins and Mestchian, 2006]. For example, both ERM and PM operate on a strategic level with the objective of increasing the likelihood that the organization's strategy is ultimately achieved. Take e.g., a view at the COSO ERM - Integrated Framework and the PM framework of Rouse and Putterill [COSO, 2004, Rouse and Putterill, 2003], both start with defining strategy, vision and objectives. Furthermore, both must be driven from the top of the organization. At last, both are designed to be ongoing, continuous processes. Namely, PM pursue continuous improvement, while ERM constantly evaluates and monitors risks [Beasley et al., 2006].

Broady & Roland discuss the link between PM and ERM by taking a step back and take an abstract view. "The goal of both PM and ERM is to monitor activities and then provide information to help improve their effectiveness, efficiency, and form" [Broady and Roland, 2008]. Both collect data that summarizes the activity of the business processes of the organization.

In both cases, after information is gathered and analyzed, a process of informing stakeholders may be initiated that reports on the failure or success of the business process in achieving the organization's objectives. In this way, "the information collected by both leads to the creation and execution of new processes for reporting and problem resolution" [Broady and Roland, 2008]. As depicted in the framework of Rouse and Putterill, stakeholders influence all levels of the organization [Rouse and Putterill, 2003]. Their requirements and expectations define environmental and general constraints that the organization must recognize in its operations.

Often improvements of the risk management approach are promoted based on the goal of "keeping the management out of jail" [Datar and Alles, 2006], but this narrow perspective obscures the larger added value of ERM for PM. As seen enterprise-wide risk and performance management are so similar and have so many overlapping aspects that an organization can benefit from a combined approach. For example, with a combined approach, PM measures an organization's progress towards achieving strategic objectives and continuous improvement, while ERM helps organizations think through positive and negative factors that can affect the achievement of these objectives [Beasley et al., 2006, Oracle Corporation, 2009]. Summarized, ERM and PM are ensuring that risks and performance are in balance, as illustrated in Figure 10.

Figure 10: Risk and Performance in balance.

COSO underpins this figure with the following statement: "value is maximized when management sets strategy and objectives to strike an optimal balance between performance and related risks, and efficiently and effectively deploys resources in pursuit of the organization's objectives" [COSO, 2004].

We will try to create a better understanding why risk and performance should be in balance by means of an example.

Example. *If an organization wants to increase the number of produced products a day, this strategy may cause risks related to the achievement of the objectives of the organization. Therefore, the organization should beside its performance think about its risks and how they can be monitored and managed. Risks in this example could be: a low stock level, lower product quality, or more loses of raw materials.*

The risks in the example should be managed, because with this strategy, the number or produced products will increase, but the organization may not benefit from it. For example, it loses to much raw materials. Therefore, managers should find a balance between the management of performance and risk.

Perhaps the most profound benefit which can be created with ERM is a sense of reliability of PM data. Management strives to look at a PM tool that reflects the current state of the organization [Broady and Roland, 2008]. When using for example, a BSC to measure performance, management defines KPIs which will be measured every quarter, year, etc. These measures help management in a manner that supports the organization's overall strategy and objectives [Nigrini and Johnson, 2008]. It is important that a PM dashboard provides the management with reliable measurement information, as unreliable measurement information may cause wrong decision making.

Example. *Imagine: an organization wants to measure the number of paid products in stock. Such a measure is dependent on several factors which can make the measure unreliable. For example, the three-way match control does not work as prescribed, which makes it possible for one and the same person to do the purchase, do the goods receipt, and do the payments of products. In this way the procure-to-pay process is not reliable anymore, because the person can, e.g., take products home without anybody noticing it. When the procure-to-pay cycle is not reliable, the measurement will also lose its reliability. I.e., the result of the measurement is 80 products in stock, but the organizations paid for 100 products. This reliability can be enhanced with ERM by managing that the three-way-match is working as prescribed, giving greater assurance that the procure-to-pay cycle is in control.*

In the example above, you can see that measuring reliable KPIs is essential for a management that wants to see how their organization is performing [Nigrini and Johnson, 2008]. ERM can give the management continuous assurance that a PM tool like the BSC is measuring each month, quarter or year reliable KPIs. By using ERM in combination with PM, management will receive a reliable answer on the question: How are we performing?

To what extent it gives reliability depends on the number of risks that could affect the reliability of the KPI and to what extent these risks are managed. The management of the organization should decide which risks are of highest relevance to manage, e.g., by following the components of the ERM framework [Broady and Roland, 2008].

With adequate, dynamic information on both performance and risks, top management has all the information it needs to decide if and when a modification of strategy, objectives, or procedures is appropriate [Beasley et al., 2006]. We think that important decisions should not be taken just from a performance perspective, but should also include the risk dimension. Ernst and Young give a good metaphor to create understanding of the need for an integrated approach:

Metaphor. *Management basing its strategy only on performance criteria is like a group of sailors setting out with a good map, compass, GPS and speedometer, but with no weather forecast, spare parts, tools, first-aid kit or life jackets.*

The sailors may be lucky and get to the right harbor on time. But then again, they may arrive too late, they may arrive at the wrong harbor or, in the worst scenario, they may never be seen again [Ernst & Young, 2009].

Managing risks beside managing performance has an important additional advantage: it helps to ensure that risks are detected and taken into account before they show up in the financial figures of an organization. Most risks however, do not start out as purely financial risks, but in other areas. KRIs in those non-financial areas are often more relevant, as they precede financial problems. In other words, non-financial indicators are often leading, whereas financial indicators are often lagging.

6.3 CA & CM and PM

As discussed in previous sub-sections, CA & CM have the potential to be of added value for ERM, and ERM should add value to PM to keep risk and performance balance. This sub-section elaborates on the extend to what CA & CM can be of added value for PM.

CA & CM's most important benefit for ERM is providing the management with accurate data and timely reporting of the organization's key risks. Indirectly this benefit can also be of added value for PM, as illustrated with the vectors from CA & CM via ERM to PM in Figure 9 at the start of this section. For example, with a combined approach organizations can improve the speed of the business. If you know that you have an accurate view of the performance and risks of your organization, you can seek for the boundaries of the business and let everything run faster. If there are any problems during this process, organizations will find it out immediately due their CA & CM activities. As Broady & Roland state: PM and ERM turns the lights on and allow organizations to see opportunities, obstacles and risks sooner [Broady and Roland, 2008], especially with the help of CA & CM tooling. On the basis of the studied literature, we see potential for CA & CM to ensure the *timeliness*, *completeness*, and *accuracy* of PM information. In the next paragraph, we present an example of Broady & Roland that illustrates how CA & CM and ERM add value to PM.

Example. *Imagine that you work in a manufacturing firm and that your ability to produce certain products depends on delivery of components from suppliers. As part of your ERM program, you institute a search for concentration in specific suppliers of key components so you can identify potential risks. The fewer the number of suppliers for a given component, the more power they will have over the organization (the more dependable the organization is). In the traditional approach to ERM (without CA & CM), you might have analysts examine the bill of materials for products being manufactured, enter the key components into a spreadsheet, sort them by supplier, and then identify the suppliers that pose the most risk. Then a program could be initiated to find alternative suppliers. For that moment in time, you understand your supplier concentration and have mitigated the risk. An approach with CA & CM would recognize that*

the concentration of risk in suppliers will change over time. Identifying and managing concentration would be made part of routine operations. Here is how this might work:

- *the bill of materials for each product would be extracted on a monthly basis into an automated report that would sort the components by supplier to reveal any concentration. Concentrations above a certain level would trigger an event that would notify the appropriate management;*
- *the report and any events would be reviewed during a monthly ERM meeting to determine how they should be re-mediated;*
- *the task of finding a new supplier, redesigning products to reduce concentration, or improving the service-level agreement with the supplier would be assigned to the appropriate management;*
- *product design staff would be part of the team managing concentration so that new product design could be performed in such a way to avoid excessive concentration in one supplier.*

In this example, the management of the specific risk (supplier concentration), has become part of an improved process that provides the organization with more information about supplier concentration to meet PM objectives and has baked ERM with CA & CM processes into standard operating procedures [Broady and Roland, 2008].

There are more advantages for PM when using CA & CM in combination with ERM. In Sub-Section 6.2 it is quite obvious that ERM and PM are in fact two halves of the same coin, both operating at the strategic level. Therefore, we think indicators used for PM may be used as indicators for ERM and vice versa. In PM, KPIs are defined and in ERM some of those indicators may be used to identify and manage risks. Only then, these are expressed as risk indicators. They are usually numbers that can be used for many purposes if they are meaningful. If these KRIs are located at the operational level and addressed by underlying automated controls (KCIs), they can be monitored with CA & CM tools. Although, this means that organization's should aggregate the performance and risk indicators from the strategic to the operational level where they may be expressed as control indicators. We will explain this by means of an example:

Example. *Imagine: in organization X, the management wants to measure the number of days they pay vendors in advance. They set a KPI for this measure and manually monitor it each month. It is beneficial for organizations to pay vendors as late as possible (a date, often set in the contract), since organizations will receive interest from the days the amount of money is on their bank account. When a performance indicator can be substituted with a risk indicator that is addressed by underlying automated controls, CA & CM tooling can continuously monitor and provide the management with up-to-date, accurate information about that specific risk and performance indicator. For example, when*

using CA & CM, organizations can align the components of the procure-to-pay cycle so they do not pay vendors in advance of the terms allowed by the contract. CA & CM enables the organization to monitor indicators like: the date of the purchase, the date of goods receipt, the date of payment, to ultimately align its payments with the contractual terms.

In the example above, from a performance perspective, the measurements help determine what the current performance is and how close or far the organization is from its expected scenario. From a risk perspective, the measurements indicate magnitude of risks that the organization faces. From both perspectives, having a clear picture allows the right remediation to be taken in a timely manner [Alles et al., 2006a]. By monitoring KCIs with CA & CM which are aligned to parent KRIs as substitution for the KPIs, there is to some extent a direct link between CA & CM and PM as depicted in Figure 9.

6.4 Concluding

On the basis of the studied literature we conclude that CA & CM has potential to contribute to both, enterprise-wide risk and performance management. Nevertheless, organizations will need a clear picture of the ways in which CA & CM would enhance their current risk and performance activities, and the barriers they may face to maximize the potential benefits. Figure 9 at the beginning of this section depicts how CA & CM can add value to PM (directly and indirectly via an enterprise-wide approach to risk management (ERM)).

The next part describes the practical situation at three Dutch organizations on the basis of the information gained from interviews with employees and experts. This Sub-Section discusses "how to determine if CA & CM add value to PM in these organizations?", to ultimately get appropriate interview questions.

Sub-Section 6.1 elaborated on the extent to what CA & CM can be of added value for ERM. But how to determine if CA & CM is doing so in practice? According to the literature from Coderre, Broady & Roland, and Deloitte, to determine if these activities can contribute to ERM, management or auditors will need to consider whether the existing controls are the most effective controls to address the parent risks [Coderre, 2008, Broady and Roland, 2008, Deloitte Development LCC, 2010]. In other words, management or auditors will need to consider whether the KCIs at the operational level address the parent risk indicators, and if these KCIs are monitored with a CA & CM tool. Variables which should be considered to answer this question are discussed in Sections 3 and 4. Concluding, we can determine the extent to what CA & CM add value to the risk management of organizations, by assessing if the current risk indicators are aligned to the underlying control indicators monitored with CA & CM tooling.

In Sub-Section 6.2 we elaborated on the quotation of Beasley et al., "PM measures an organization's progress towards achieving strategic goals, while

ERM helps company leaders thing through positive and negative factors that can affect the achievement of their goals" [Beasley et al., 2006]. They are in fact two halves of the same coin, both operating at the strategic level. In other words: "performance indicators should be measured to manage the progress toward achieving the organization's objectives, while risk indicators are measured to manage the factors that can affect the achievement of those objectives" [Nigrini and Johnson, 2008]. As Ernst & Young state: "a KRI should be expressed in an unit of measurement that is predictive for the KPI to which it is linked" [Ernst & Young, 2010]. When organizations implement their RM approach according to COSO's ERM - Integrated Framework and their PM approach according to the framework of Rouse and Putterill, then the KRIs should align the KPIs [COSO, 2004, Rouse and Putterill, 2003], because both frameworks define indicators according to the organization's strategy and objectives.

In addition to that, the selected set control indicators should address parent risk and performance indicators. But as discussed earlier, PM and ERM operate at the strategic level, while CA & CM are best considered in the context of monitoring activities at the operational level [Deloitte Development LCC, 2010]. So this requires organizations to aggregated risk and performance management from the strategic, to the operational level, if they want to add value to both with CA & CM. Therefore, management should give careful consideration to what control indicators should be measured (do they address parent performance or risk indicators?), how they should be measured, where the necessary data resides and the quality of the data. As Alles et al., state: "simply switching on rules that may exist within the technology tools without refining them could result in an unmanageable number of exceptions and false positives requiring attention, in turn resulting in increased inefficiencies as well as false information and wrong decision making. Similarly, switching on poorly designed rules may not properly identify exceptions associated with risk and performance, and may lead to the same wrong decision making" [Alles et al., 2008].

Concluding from this, we can define questions like: Do organizations take an enterprise-wide approach to RM? Is PM aggregated throughout the organization? How are the KCIs defined? Are the KCIs of CA & CM addressing the risks managed with RM? Which kind of risks do they address? Are the KRIs of RM aligned with the KPIs of PM? In which processes do they address them? Etc. For details about the interview questions, refer to the interview framework in Appendix C, Sub-Section C.4.

In this interview framework we distinguish two different types op business processes. The following definition of a "business process" of Rummler & Brache clearly accentuates these:

> *"a business process is a series of steps designed to produce a product or service. Most processes are cross-functional, spanning the white space between the boxes on the organization chart. Some processes result in a product or service that is received by an organization's external customer. We call these primary processes. Other processes*

produce products that are invisible to the external customer but essential to the effective management of the business. We call these secondary processes" [Rummler and Brache, 1995].

The above definition distinguishes two types of processes: primary and secondary processes, depending on whether a process is directly involved in the creation of customer value, or concerned with the organization's internal activities.

This section showed that from a theoretical point of view CA & CM have potential to add value to PM. The next part elaborates on the practical sight of the story. We interviewed employees of three Dutch organizations and three experts of KPMG about: the current situation of CA & CM, RM, and PM; if and how CA & CM add value to PM; and their view about the theoretical findings as discussed in this section.

Part IV
Practical Findings

With the model defined in Part III, the practical part of this research is about to begin. This part provides the reader with information about the practical situation at two organizations in the Netherlands which implemented CA & CM a few years ago and one organization in the Netherlands with strong RM and PM activities. We furthermore interviewed three experts of KPMG on the area of CA & CM, RM, and PM; and visited two seminars about CA & CM. This section also describes the interviewees' view about the theoretical findings as described in the previous part.

Contents of Part IV

7 Perceived Added Value of CA & CM from a Practical Perspective

We interviewed employees of three organizations and three experts on the basis of the interview framework presented in Appendix C. The objectives were to:

- determine the current situation of CA & CM, RM, and PM;
- determine the current relations between CA & CM, RM, and PM;
- determine the current added value of CA & CM for PM;
- get the interviewees' view about the theoretical findings as described in Part III.

The interviewees of the three Dutch organizations come from a lifting and transport organization (A), an international life science and performance materials organization (B), and a governmental agency (C). In this research we will express the organizations as "organization A, B, or C".

In addition to these interviews, we interviewed three experts of KPMG: one on the CA & CM area, one on the RM area, and one on the PM area. We will mention them as "... expert". For example, if we talk about CA & CM, we will express the expert as "the CA & CM expert".

Furthermore, we visited two seminars about CA & CM. The information gained during these seminars shall be used to create information completeness. For details about the interview framework please refer to Appendix C.

This section discusses per situation: the current situation of CA & CM, RM and PM, how they are related, and the added value perceived from these relations. As additional information, it describes the experts' view about the theoretical findings of Part III. The paragraph names used in the sub-sections correspondent with the paragraph names of the interview questions in Appendix C.4.

7.1 Case 1: Organization A

Profile Organization A is a specialist in heavy lifting and transport solutions at any onshore or offshore location. The global/international company is family-owned and Dutch in origin and has approximately 4000 employees worldwide, of which approximately 1000 are employed in the Netherlands and the other 3000 working from almost 70 other locations around the world. Global or complicated projects and worldwide logistics are handled centrally from their home base in the Netherlands. The current turnover at the moment of writing is around 1 billion Euro. A started with their CA & CM initiatives about two years ago to get insight in the operating of the effectiveness of internal controls related to their common and centralized SAP system.

CA & CM When we started to explain CA & CM at organization A, the interviewee directly intervened and explained that they only use CM and not CA to monitor four secondary processes: purchase-to-pay, finance-to-report, order-to-cash, and projects. It is using the SynAxion tool (Appendix A.6) to monitor 28 KCIs which are selected out of 100 indicators, based on ease of implementation and priority. Every month, each Business Unit (BU) reports these control indicators to the holding. The holding on its turn, analyses and reports them back to all units. Despite the fact that it are only 28 indicators which are monitored automatically, it takes a large amount of time, energy, and resources to analyze and report them back. For that reason they want to decrease the reporting frequency from ones a month, to ones a quarter.

The control indicators are related to business process controls located at the operational level. Examples included: the number of open down payments vendors, the number of open down payments customers, the number of changes to vendor bank accounts, and the number of duplicate vendor master data.

Organization A uses the SynAxion tool for all BUs. This is possible because its secondary processes are IT-facilitated and have a centralized and standardized structure. In contradiction, the primary processes are not, or to a limited extent IT-facilitated, centralized, and standardized. According to the interviewee of A, "therefore, these processes are not monitored with the CM tool".

The corporate controller is responsible for the CM activities, because A does not have an internal audit department. The corporate controller uses the term "KCIs" to accentuate control indicators which are currently monitored with the SynAxion tool.

RM Originally, A is a family-owned company and during the interview it became clear that RM is not drilled down into the organization. According to the interviewee, "risk is not embedded in their culture". Every process has its own risks and most of them are monitored, automatically or manually by process owners. The connection between these risks is usually missing and not related to the organization's objectives. Furthermore, the objectives of the BUs do rather address the objectives of parent BUs, or the objectives of the entire organization. "We are managing risks, but not according to a prescribed or common framework".

We defined four categories of risks in Section 4. Organization A addresses two (financial and compliance) of the four categories. The interviewee stated: "the management of strategic and operational risks should be improved in the future". For example, the core strategic risk of organization A is "safety". Safety is a strategic risk, because it can affect the brand/reputation of the organization. This risk is important when performing the core primary processes: lifting and transport, i.e., a lack of safety during a lifting process can have huge consequences for the organization. Consequences could be: injuries, death, and/or a loss of reputation. You should expect that A strictly monitors and manages such risks, but surprisingly it is not! According to the interviewee,"the managing of these safety risks can use some improvements". For instance, he stated that

too often employees take the "quick and dirty" approach, instead of working according to, and with, the safety standards and safety equipment.

Although A should monitor and manage such risks, it is also creating value with the current risk management approach. Customers of organization A value this approach, as it is part of the culture of the organization. Nevertheless, the interviewee stated that the responsible management are lagging in an iterative approach to it. The KRIs are at the majority of the BUs not assessed or evaluated, which may create a false sense of, e.g., safety information. He confirmed our statement, that risk indicators should be evaluated in the future to ensure that the right indicators are managed to ultimately get a reliable view about the core risks the organization faces.

PM Despite the fact that A does not use any method described in this research to manage its performance, it does report strategic KPIs to the top management. Every quarter, the BU managers report the holding about the following financial performance indicators: solvability rate, interest coverage rate, total debt to EBITDA, return on capital employed, and return on average equity. These are partly monitored on an automated basis, however, employees still need to put them manually into spreadsheets. Beside these financial indicators, organization A monitors two non-financial ones: progress of the order book and the planning of the thirty biggest cranes.

Despite this, there is no common framework in place for reviewing the information generated. The interviewee partly confirmed our statement about the unreliability of the performance results: "the existing tools may not provide sufficient, relevant information and feedback in terms of what is happening within the company or why it was happening, nor do they effectively drive consideration of what their organization needs in the light of the information to ensure successful execution of business objectives and financial performance". According to the interviewee, therefore, they may start a research to find those key operational success factors that might lead to financial performance in the future.

Added Value CA & CM for PM According to the interviewee of organization A, the CM tool of his organization is to a limited extent adding value to their RM activities. The control indicators which are monitored by SynAxion are aligned with the risk indicators, but only for the secondary processes. As described, organization A has well researched the controls which address the parent risks, but because it is only monitoring the secondary processes, there still is a gap for the risks at the primary processes which do not have underlying control indicators in place. This means that the main risks, the ones that can prevent the organization from achieving its strategic objectives are not, or minimally monitored and managed.

According to the interviewee, the monitoring and managing of these primary process risks should be improved, but he also stated that this is not as easy as it seems to be. Due to the fact that the KRIs of the primary processes are to

a limited extent linked to an IT system or addressed by automated controls, SynAxion cannot access this data from the SAP system. This in contradiction to the secondary processes, which are facilitated by the SAP system, and where the majority of the transaction information is collected in the SAP database. The interviewee agreed on our conclusion, "SynAxion monitors the compliance and financial risks, but only the ones of the secondary processes".

We listed the KPIs of organization A at the beginning of this sub-section. The interviewee stated: "it will be hard for this organization to translate these to KRIs at the operational level". According to him, the main cause to this is the approach they take to RM and PM. For example, organization A knows that its main risks are at the primary processes, but take a fragmented approach to solve them. Managers generally are looking at these risks, but they are using their own tool, vocabulary, and terminology to manage them. And as the interviewee states: "this terminology and vocabulary is often very informal". PM measures the organization's progress towards achieving strategic objectives and continuous improvement on financial performance indicators, but the current RM approach does not manage those positive and negative factors that can affect the achievement of these objectives.

This is according to the interviewee also the reason why it is almost impossible to monitor strategic performance indicators with SynAxion. Their PM activities are to a limited extent systematically aggregated throughout the organization and furthermore the strategic risks of organization A are located at the primary processes which are rather facilitated by IT. Concluding, at the moment there is no direct relation between the KCIs at the operational level and the KPIs at the strategic level.

Despite the fact that there is no direct relation in the organization, there is an indirect relation between CA & CM and PM. The indicators monitored with SynAxion are derived based on the key risks at the secondary processes. These can be seen as performance indicators at the operational level, because they contribute to the PM of the secondary processes. For example, at organization A, SynAxion ensures reliability of the performance information at the secondary processes, because risks at these processes are managed and underlying controls are monitored.

7.2 Case 2: Organization B

Profile Organization B is an internationally operating company with more than 200 BUs in 49 countries throughout the world. B has a decentralized organizational structure built around business groups that are empowered to carry out all business functions. It has approximately 23000 employees worldwide, of which approximately 7000 are employed in the Netherlands. The current turnover at the moment of writing is around 9 billion Euro. Currently, B has started a CA & CM project and is probably going to implement SAP GRC Access Controls and Process Controls (Appendix A.1).

CA & CM Organization B's industry best practices constituted the foundation for their Key Control Framework (KCF), which includes controls for the standard business processes: order-to-cash, purchase-to-pay, finance and controlling, and service management. This KCF is the basis for the common internal audit approach, as well as the external audit approach. To strengthen the common audit approach, A started with automating the monitoring of process controls. KPMG has a quality assurance role in the design and testing phases of all KCIs and selection of the CA & CM tool, which will be specially tailored to the organization.

Organization B will probably implement one CA & CM tool for every BU, because of their decentralized IT structure. The secondary processes in these BUs are standardized, but the current tooling used in these processes is divergent. Every BU of organization B has its own SAP system, which requires B to implement one CA & CM tool per BU. Although, currently they perform a research about the possibilities to change the decentralized IT structure, to a more centralized one. The interviewee stated: "in this way we are more likely to succeed in leveraging our investment in CA & CM across the entire organization".

The organization has an internal audit department responsible for the audit activities. Despite, the BU's management will become responsible for the CA & CM activities. They will report to the internal audit department about their key controls. The internal audit department provides assurance over the BU management's control and monitoring capabilities.

RM The managing board of B is responsible for RM and has designed and implemented an ERM system. The aim of the system is to ensure that the extent to which the organization's strategic and operational objectives are being achieved is understood, that the organization's reporting is reliable, and that the organization complies with relevant laws and regulations.

The system is based on the COSO ERM - Integrated Framework. According to the interviewee, it aims to achieve maximum integration of the RM processes into the normal business processes. The internal controls for the goods and money flows have been built into standard business processes and tools have been developed to support their implementation and to monitor their effectiveness in operation. The interviewee stated: "in this way, a high level of internal control can be achieved efficiently".

All BUs have an audit committee, which under the direction of the BU's management sets up annual RM plans, monitors their implementation, and reviews risk issues on a regular basis (once a quarter). Major RM events, such as the outcome of corporate audits, business risk assessments, and the occurrence of material control failures or weaknesses are discussed with the responsible management. Based on development within and external to the organization, as well as the findings from the monitoring activities as described above, the risk management approach is regularly adapted and optimized.

Organization B divided risks into two categories: the generic ones and the

BU specific ones. They have crystallized processes to manage the generic ones and all BUs should take this standardized approaches (to a great extent automatic). The high priority generic risks are: the impact of the global financial crisis and economic downturn; disposals and acquisitions; price volatility of raw materials and energy; deteriorating market conditions; the ability to turn innovation efforts into profitable business; and the people, organization and culture. Furthermore, every BU has its own BU specific risks, that at the majority of the BUs are risks of the primary processes. There are no standardized processes or approaches to manage those, therefore the accountability falls to the BU's management. The approach they take to manage those risks is most of the time BU specific.

PM When we asked the interviewee about the PM approach used, he answered that there is no common method used. Although, the PM approach B takes is based on the BSC (Appendix B.3). The interviewee stated: "in some organizations the PM processes are fragmented and supported either by spreadsheets or point solutions. We have thought about these processes holistically and adopted a suite of applications and a platform to integrate the management processes".

The top management requires every BU to report, each month, a number of strategic financial KPIs. Beside these financial ones, they are also monitoring non-financial performance indicators. Nevertheless, the core KPIs are purely financial: net sales, total debt to EBITDA, EBITDA / net sales, operating profit (EBIT), return on capital employed, capital expenditure and acquisitions, R&D expenditure, and workforce. When we asked why?, the interviewee stated: "whereas failing to meet non-financial targets may not be treated as a great crime, failures to hit financial targets are more serious".

According to the interviewee, "for a PM method to have real impact upon the running of an organization, it is important that the information gained drives actions and change. A clear ownership of the management system and subsequent results are key factors in this success". In organization B, the management of the BU is responsible for the PM activities. They report to the top management about their BU's performance.

Added Value CA & CM for PM As noted above, B is in the middle of a CA & CM project in which they are searching for the best tool to monitor the KCIs of the KCF on a more frequent and automated way. Despite the fact that they are searching for new ways to monitor the KCIs, the interviewee stated: "the current financial reporting provide a reasonable level of assurance that the financial reporting does not contain any material inaccuracies, and confirms that these controls functioned properly in the year under review and that there are no indications that they will not continue to do so. The financial statements fairly represents the organization's financial condition and the results of the organization's operations and provide the required disclosures". In view of all of the above, the interviewee confirms that the current KCF adds value to the

reliability of the performance data and that financial statements give a true and fair view of the financial figures.

Despite the fact that to the knowledge of the interviewee the KCF ensures reliability, B is searching for ways to enhance this reliability and especially the efficiency of the monitoring activities. Not all indicators of the KCF can be monitored with CA & CM, because some are manual. At organization B, most information is located in databases, but they have problems defining which information is most important to monitor. The interviewee of organization B states: "the identification of risk indicators and assessments are key task which many organizations underestimate. Getting the right data is a critical juncture in the implementation of CA & CM".

In organization B there is a strong linkage between PM and RM activities. The KRIs and KPIs are aligned to the objectives of the organization. In this organization, performance and risk management have the same ultimate goal, ensuring the achievement of the organization's strategic objectives. He stated: "our PM is focused on ensuring that good things occur as planned, while our ERM is typically focused on ensuring that bad things do not occur".

At the moment, there is no direct relation between the KCIs at the operational level and the KPIs at the strategic level. According to the interviewee, "the KCIs do not provide the management with performance information. Nevertheless, the indicators of the KCF do ensure reliability of performance information".

According to him, CA & CM should increase this reliability and especially the efficiency of the monitoring activities, but there are some important factors to think about before organizations start implementing such a tool. He stated, "to what extent CA & CM can be of added value for PM depends on a number of factors: the percentage of IT facilitated processes, the extent to what an organization have a standardized IT infrastructure, the extent to what an organization takes an enterprise-wide and systematic approach to PM and RM, and the extent in which the project is supported by the top management and the rest of the people in the organization".

Finally, we will accentuate a statement of the interviewee of organization B: "the monitoring of KPIs should be a key component of the RM and control programs. With an integrated, principles approach to managing compliance, risks, and performance, organizations can grab with greater confidence the opportunities that the current economy presents".

7.3 Case 3: Organization C

Profile Organization C is a Dutch governmental institute which promotes legal certainty in transactions involving registered properties. With its decentralized structure, C operates as closest to the citizens. It has approximately 2000 employees which are all employed in 9 BUs in the Netherlands. The current turnover is around 245 million Euro. At the moment of writing this thesis, C does not have a CA & CM system.

CA & CM It is organization C's objective to pay more and closer attention to the wishes of their clients. Information and communication technology are making it increasingly easier to put the organization's information and products available online via the Internet, for both private citizens and organizations. According to the interviewee, it is recognized as one of the most innovative government bodies that make use of the Internet. Today, 45000 professional users make use of their services every day and over 100000 information products are provided in a digital form. With this growing usage, protecting the organization's infrastructure from information theft and complying with regulations while ensuring users' privacy has become essential to organization C and its services. As has the need to continue to provide the information in a correct and effective manner. So we asked the interviewee, why does organization C not implement CA & CM to enhance this process? This question will be answered in the next paragraphs.

RM When we asked the interviewee about the framework used for their RM activities, he answered: "we are not using a common framework like the COSO ERM - Integrated Framework". Despite that, they are addressing mostly of the components of the framework. C takes an enterprise-wide approach to RM, which according to the interviewee can be expressed as ERM. Their ERM is systematically developed and aggregated throughout the organization. Organization C faces risks and uncertainties in carrying out their operations and achieving their objectives. They take measures to manage their risks and uncertainties, having identified a number of high-risk areas (in secondary and primary processes) which could prevent the organization from achieving these objectives. The risks and measures taken to address them are periodically, once a quarter, evaluated by the management.

According to the interviewee, ERM approaches will likely vary from organization to organization. He stated: "in fact there is no universally ideal ERM approach for a particular organization". This is the reason why organization C is only using some components of the framework to manage their strategic and operational risks, instead of using the complete set of components.

These strategic and operational risk indicators are rather monitored on an automatic basis. They have partly automated the monitoring with a range of tools, but still manual effort is needed. Despite the fact that risk managers are responsible for these monitoring activities, they lack in an iterative approach to it. He stated: "risk managers should regularly review progress in the implementation of activities chosen to deliver the organization's objectives, including the activities as part of the risk review. Risks change constantly and new risks emerge while old ones fade in importance, and existing risks rise and fall as business conditions change". According to him, risk monitoring is required to: ensure that assurance is provided on today's more relevant risks; identify new or growing risks that require additional risks and control monitoring; identify sudden risen in risk levels that may need immediate attention by management or internal auditors.

PM Whereas organizations A and B send a spreadsheet with KPIs to the top management, organization C takes another approach to PM. It uses a range of tools to assess and improve the quality of its operations and the organization as a whole. Their main PM tool is the Quality Charter (QC). The charter contains standards relating to product quality, speed of delivery and the handling of complaints, among other issues. There are three main service lines which report once a quarter to the top management. In contrast to the other two organizations, they publish this QC and make it accessible for everybody interested in their business. The interviewee stated: "this allows customers to hold this organization to its stated delivery times and stated quality levels for its products. On the other side, this drives this organization to increase its performance and PM quality".

The QC contains only non-financial KPIs: complaints and objections, delivery times, and quality of registered records. These KPIs are translated to operational metrics, and a norm is set for each metric. The results of the metrics are, once a quarter, reported to the top-management and other stakeholders (e.g., employees).

C developed its PM approach based on the strategic objectives of the organization and takes an enterprise-wide approach to it. The interviewee stated, "successfully implementing a PM program requires an approach that flows from a strategic plan, measures progress against carefully defined objectives and rewards stakeholders for behavior and actions that meet those".

With the help op KPMG they keep track of their most important KPIs. For instance, KPMG just started a research about the quality of the QC in which they assessed the effectiveness of the set of KPIs. According to the interviewee, to provide continuous improvement, this organization performs periodic strategic reviews and appropriate adjustments in the strategic indicators and their underlying operational metrics.

Added Value CA & CM for PM At the start of this sub-section we elaborated on the need for organization C to protect the organization's infrastructure from information theft and complying with regulations, and asked why the organization does not implement a CA & CM system to enhance this process.

The answer to this question is quite simple. According to the interviewee, "the efficiency of a CA & CM tool depends on the ease with which monitoring can be built into the daily process of each line of business. This requires that the processes with the highest risks, or the most important performance metrics, are IT-facilitated". Nowadays, employees of organization C are monitoring the greatest part of the KCIs of the primary and secondary processes by hand.

This is the main reason why organization C is to a limited extend interested in CA & CM systems. They have no common, centralized ERP system and the majority of their process information is not automatically collected in their systems.

Despite the fact that they do not monitor on a continuous and automated basis, their risk and performance management approaches are in balance. Ac-

cording to the interviewee, "RM without an effective strategic PM to provide the context for risk evaluation will in the best case provide only limited value and in the worse case can misguide the organization's control efforts, possibly even obscuring more important strategic risks". He stated, "every organization must, in addition to defining the key indicators for success, also define its critical failure indicators. That are those circumstances under which the organization is no longer likely to be successful".

Although the fact that this organization does not have a CA & CM tool, the interviewee sees potential for such tools in this, and other organizations. "If organizations can translate these failure indicators to metrics which can be monitored with CA & CM, these metrics then serve as an early warning mechanism thereby allowing the organizations to restructure a process before good resource and money are thrown after bad".

7.4 Additional Practical Information

Profile This sub-section contains information gained from the interviews with experts and from the visited seminars about CA & CM. The next paragraphs will only describe that information we think can be of added value for this research.

CA & CM Organizations B and C do not, or to a limited extent have a centralized structure and information is spread in many places across the organization. Also other organizations have such decentralized structures. For instance, an employee of a car leasing organization in the Netherlands stated during one of the seminars: "we have a strongly decentralized structure, with more than 30 BUs, all with their own RM approach. Furthermore, we have different obsolete legacy systems, so it will be hard to implement an efficient CA & CM tool in this environment".

Another issue discussed during the seminars is: who should be responsible for CA & CM? According to the CA & CM expert, CA should be performed by the second or third line of defense (preferably, internal auditors), and CM activities should be performed by the first line of defense (management). But in practice, accountability for CA & CM typically falls to other stakeholders.

The discussions during the other seminar underpin the responsibilities as stated above, but also accentuate on an evolving process to get the support from the management to perform CA & CM. An employee of KPMG stated: "most of the times, the internal audit department starts with CA & CM initiatives. The management in their turn notices the nicely generated reports with information they could use in their decision making. This ultimately triggers them to start using the CA & CM tools, or its outcomes".

According to an employee of a Dutch electronics company, "by implementing monitoring activities as CA & CM, the level and type of day-to-day work performed by internal auditors will change and it will involve more and deeper discussions with management about the business, its risks, and controls". As the CA & CM expert stated, "internal auditors will be recognized as value

adding contributors, so that both the work will be more interesting and the recognition for their effort will be much greater". During the interviews at the three organizations, we noticed that the terminology used by the interviewees is very divergent. We asked the CA & CM expert about the different ways organizations express the indicators of CA & CM. This resulted in four different definitions: Key Integrity Indicators (KIIs), Key Performance Indicators (KPIs), Key Control Indicators (KCIs), and Key Risk Indicators (KRIs).

RM According to the RM expert, the monitoring of risk indicators at the majority of the organizations is performed monthly or quarterly, but usually not on an automated basis. At most organizations, spreadsheet tools like Excel are manually filled with risk information. According to him, "RM should be part of the culture and the support should start at the top of the organization. Unfortunately, this is often not happening in practice".

You have seen the difference between the approaches the three organizations take to RM. Despite the fact that organizations B and C do take a systematic approach, still there could be some challenges for such enterprises. The RM expert determines some challenges in practice to evolve organizations' risk assessments and audit activities continuously, to keep them aligned with developing risks, and to ensure that those risks are addressed in a timely basis, thereby helping to drive a fully risk-based approach. For example, if the government creates new laws and regulation, controls will change. But according to the expert, "a great majority of the organizations are not, or to late responding to such changes/events".

During the interview with the expert, we explained the "risk appetite" problem of organization A. According to the RM expert, for such organizations it is hard to define the "risk tolerance" and "risk appetite". He accentuated that they must find a balance between those two, to satisfy the customers, and ultimately create the maximal benefit.

PM In the three cases described in this section, non of the organizations is using the BSC. The PM expert underpins this practical conclusion, he stated: "most organizations' PM approaches are more or less the same as the BSC, or based on the perspectives of the BSC". According to the PM expert, the majority of the organizations report their KPIs each month or quarter, with some exceptions who want to know their actual performance on a weekly basis. In comparison with risk information, at most organizations spreadsheet tools like Excel are manually filled with performance information.

The PM expert accentuated on the processes underlying performance. "Understanding the processes underlying performance is the only way to define the indicators and metrics that lead to actions. If organizations understand which of the steps in the process is defective, appropriate correcting actions can be identified. If, however, only the final, high level indicator (e.g., net income) is looked at, no appropriate correcting action can be identified". When we asked him about the terminology used to express the indicators of performance, he

answered resolutely: KPIs. Also during the seminars, the term KPIs was used to express performance indicators.

80 percent of the KPIs in practice are financial ones, but the PM expert thinks this will change in the next five years. He once asked a Dutch prison manager the question about, whether the financial KPIs really reflected the most important aspects of the organization's performance? He received the following answer: "I think our annual report gives a good illustration of what we do and what is important". But as he said after reading it: "the primary question has not been answered - that is preventing criminals from doing it again".

Added Value CA & CM for PM During one of the seminars, an employee of KPMG stated: "compliance-driven approaches to managing risk no longer suffice in an increasingly volatile, interconnected business environment. Approaches to RM need to provide the management with an integrated view of risk and performance that defines how rapidly emerging events will impact operations, quality, and ultimately shareholder value".

The RM expert stated: "it will be almost impossible to ensure reliability of strategic KPIs with CA & CM if you take a fragmented approach to risk and performance management. Only when organizations have fully aggregated RM and PM throughout their business, this is possible". He explains this by means of an example: "as it is popularly described in the media, PM, whether defined narrowly or ideally more broadly, does not currently embrace risk. It should! Risk and uncertainty are too critical and influential to omit. For example, reputational risk caused by fraud (e.g., Ahold), a terrifying product related incident (e.g., Toyota), more recently a media incident (e.g., T-Mobile with Youp van 't Hek), or some other news headline event can substantially damage an organization's market value.

The CA & CM expert underpins the statements of the RM expert, but determines some problems for CA & CM to add value to this process. According to him, "only if the information is located in a database and has got the right format, it is accessible for a CA & CM tool and can be monitored, analyzed and reported on a continuous and automated basis".

Part V
Concluding Findings

This part links the theoretical findings from Part III with the practical findings from Part IV. It contains an analysis about the theoretical and practical findings and furthermore describes the findings about the different topics/questions discussed in this research.

Contents of Part V

8 Synthesis of Theoretical and Practical Findings

Each of the following sub-sections includes a table with the examined characteristics expressed per organization. Three colors are used to give the reader an indication of the extent to what the organizations fulfill to the characteristics. Green and red outcomes express that the organizations fulfill or may not fulfill to the characteristic. Orange indicates that the organizations fulfill, but not completely. The indications are established on the basis of the information gained from the interviews with employees of the three organizations, and on the basis of the information gained from the interviews with the KPMG experts.

8.1 CA & CM

During the interviews, we recognized that more than likely of the organizations' key controls are manual, which by their very nature makes them difficult to continuously monitor, without hiring someone to stand over someone's shoulder. This is a "big elephant in the room" for most internal auditors or management when deciding how to be more efficient and proactive. Continuous monitoring and auditing of controls is possible and extremely efficient, but before organization's cover that, they should consider some pitfalls/characteristics we have observed in literature and during the interviews in practice. Figure 11 illustrates the core characteristics and the extent to what the three organizations fulfill to those. Only the characteristics comparable to the organizations are depicted in the figure. The others will be discussed in the subsequent explanation.

	Organization A	Organization B	Organization C
Employees	+/- 4000	+/- 23000	+/- 2000
Turnover	1 Billion	9 Billion	245 Million
Sector	Civil, Power, and Offshore	Chemical	Public
IT-Facilitated Processes			
Centralized IT Structure			
Standard IT Systems			
Automated Controls			

Figure 11: Practical Results

First, from practice we conclude that organizations are narrowly focusing their CA & CM activities on regulatory compliance. A research of KPMG at 138 organizations in the Netherlands revealed that the greatest part are starting CA & CM initiatives from a compliance perspective instead of taking a broader view about enterprise risk and performance management [KPMG, 2010b]. Com-

pliance is an important, but discrete element of RM and can result in silos of risk information that often hamper an organization's ability to monitor critical risks that can affect the achievement of an organization's objectives. Implementing CA & CM should not just be a technology exercise which is focused on regulatory compliance, but it can be seen as an opportunity of changing the type, speed, and visibility of information on control, risk, and performance that should have a significant impact on how business decisions are made and monitored.

The second characteristic we will discuss contains the thought that implementing CA & CM can be more successful and more valuable when controls have been optimized. From practice, we see that this usually requires that a minimum of 60 to 70 percent of the controls are automated. But as depicted in Figure 11, the reverse is often the case. At all three organizations, only the secondary processes have a minimum of 60 to 70 percent of the controls automated, while more than likely of the primary process controls are manual.

Third, in addition to automated controls, those that have centralized and standardized IT-facilitated processes, systems, and infrastructure are more likely to succeed in leveraging their investment in CA & CM across the entire organization. Centralizing CA & CM activities means that systems can be centrally monitored. Conversely, organizations that have a wide variety of processes, systems, data and infrastructure may have to adapt or customize their CA & CM approach every time. For example, the two organizations that do have a decentralized IT structure even may deploy different tools for their different environments/BUs. Despite the fact that organizations can be fully automated and control indicators can be measured automatically with CA & CM, there still can be obstacles related to the varied data formats used. The ability to access and retrieve data from a variety of record sources is crucial when an organization wants to maximize the benefits from CA & CM. This means that when data is in a variety of formats, with different file types and record systems, it becomes necessary to standardize this data. Unfortunately, this can be a complex, time consuming, and expensive process.

Fourth, as described in the theoretical findings, CA & CM together can deliver greater value to an organization than when they are implemented independently of each other. From practice this is confirmed by the interviewees, although, currently organization are still using one of the two.

Fifth, based on the available literature we identified the stakeholders of CA & CM and noted that CA should be performed by the second or third line of defense, and CM by the first line of defense. In practice we see that accountability typically falls to other stakeholders, depending on the size and culture of the organization.

Sixth, another important aspect we see in theory and practice is the support from the C-level executives, including the CEO, CFO, and COO. This support from executives is often necessary for auditors to obtain physical and logical access to the required information. In all organizations the CA & CM initiatives are supported by the top management, and stakeholders are enthusiastic about the new auditing approaches.

Finally, from literature we have seen lots of different definitions to express the indicators monitored with CA & CM. In addition to this, during the interviews we noticed that the terminology used in practice is also very divergent. Therefore we introduced a new definition which currently is not the standard in literature: Key Control Indicators (KCIs). We have introduced this definition, because current other terms used like KRIs, KPIs, KIIs, can lead to wrong associations relating to performance and risk indicators.

8.2 RM

We elaborated on RM in Section 4 of Part II, and stated that RM should be applied in a strategic setting, across the enterprise, and based on a common used framework. We just mentioned a few of the selected characteristics that will be discussed in this sub-section. Figure 12 illustrates the characteristics comparable to the organizations. The others will be discussed in the subsequent explanation.

	Organization A	Organization B	Organization C
Employees	+/- 4000	+/- 23000	+/- 2000
Turnover	1 Billion	9 Billion	245 Million
Sector	Civil, Power, and Offshore	Chemical	Public
Standard Methodology			
Enterprise-wide Approach			
Strategic Risks			
Financial Risks			
Operational Risks			
Compliance Risks			
Iterative Approach			
Automatic Monitoring			

Figure 12: Practical Results

First, if we take a theoretical point of view, organizations should manage their risks according to a common ERM framework. For example, according to the COSO ERM - Integrated Framework. In practice the approaches organizations take to RM are very divergent. Some organizations are using the COSO framework, while others are only using some components of it. There is also a group that takes to a limited extent an enterprise-wide approach and does not use a common framework. Such a framework may be too generic to rely on entirely, but we think that if an organization has a breach of security, they would at least be in a position to say that they have a common structure

in place. Furthermore, these frameworks can serve as an organizing principle around which organizations can develop their compliance initiatives, ensuring that all the bases are covered. But as described in Section 7, in practice such frameworks are not always used. A research of IMB underpins this finding, they conclude that only 52 percent of the organizations take a formal approach to risk management [de Schiffart, 2010]. The same research shows that organizations that put a lot of energy in managing risks are significantly more successful than those that fail in managing risks.

Second, in practice we determined a relation between the organization's size and the design and use of RM. Firm size is positively related to the adoption of an enterprise-wide risk management approach. The greater the size of the firm, the more systematic the approach to RM as depicted in Figure 12. Beasley et al., underpin this conclusion and found that the market reaction to the adoption of ERM is positively related to firm size, where the adoption of ERM is signaled by the hiring of a risk manager [Beasley et al., 2006]. COSO also notes the importance of firm size when designing ERM [COSO, 2004]. Furthermore, the approach to RM and especially the number and different types of risks managed depends on the culture and industry of the organization.

Third, a non enterprise-wide approach encompasses that organizations have no way of aggregating data about risks. Because they cannot aggregate the data, they cannot really gain a strategic enterprise-wide view of risk either. Maybe this fragmented approach to risk even creates a false sense of security. Managers think their own organization is managing risks, but in fact the organization lacks any visibility or insight into common business situations. This could be a reason why only one organization is managing all four distinguished risk categories, while the other two only manage them for the secondary processes, or manage only a few of the categories.

Fourth, organizations need to consider whether the existing indicators are the most effective ones to address the parent risks. In addition, stakeholders should give careful consideration to what should be managed and measured, how it should be measured, where the necessary data resides, and the quality of the data. They should do this periodically on an iterative basis, but as depicted in Figure 12 in practice organizations have a lot of difficulty with that job.

Fifth, from a theoretical point of the view, the risk management department has responsibility for creating the environment and the structures for RM. In practice, also the responsibility strongly depends on the size of the organization. Depending on the size of the firm the RM function may range from a manager, a part time risk manager, to a full scale risk management department.

Finally, while the terminology used to express control indicators is very divergent. The term used to express risk indicators "KRI", has been widely accepted for some time in literature and practice.

8.3 PM

In Section 5 of Part II, PM is discussed and some characteristics are selected. This sub-section discusses these characteristics and how they are embedded in

practice as depicted in Figure 13.

	Organization A	Organization B	Organization C
Employees	+/- 4000	+/- 23000	+/- 2000
Turnover	1 Billion	9 Billion	245 Million
Sector	Civil, Power, and Offshore	Chemical	Public
Standard Methodology			
Enterprise-wide Approach			
Iterative Approach			
Financial Indicators			
Non-Financial Indicators			
Automatic Monitoring			

Figure 13: Practical Results

First, in Section 5 we mentioned that the BSC is one of the most widely used PM methodologies in the world [Kaplan and Norton, 1996a]. This may be true, but we have seen that the organizations described in this research are not using such methodologies itself. They are simply using the best practices of the methodologies.

Second, all organizations are managing their performance, though it is at the end of the year during the annual audit. But not all organization are motivated by the belief that systematic approaches to it are likely to lead to superior operationalizations. We have discussed the model of Rouse and Putterill in Section 5 [Rouse and Putterill, 2003], but in practice such models are rarely used. On the basis of the practical information gained from the interviews can be concluded that the majority of the organizations base their PM activities on approximately 10 strategic KPIs, for the greatest part financial ones. Nevertheless, we expect that within the next five to ten years, every organization will have to redesign their PM activities. At the moment, the greatest part of the measurements are typically derived from, or directly related to, the chart of accounts and found in an organization's profit and loss statement or balance sheet as depicted in Figure 13. Conspicuously, one of the organizations operating in the public sector only monitors non-financial performance indicators. From this, we conclude that in profit organizations financial KPIs are leading, while they are lagging in non-profit organizations.

Third, only changing the KPIs is not enough. Somehow, an organization's strategy objectives and indicators should be translated into objectives and measures for underlying BUs and individuals. This again could be achieved by developing an organization's PM according to, e.g., a common framework like the one from Rouse and Putterill [Rouse and Putterill, 2003]. This means that at the lowest level of PM lies measurements of human performance and the overall

strategic organizational performance is the ultimate level. In between lie other layers, such as team performance, service group performance, and BU performance. We think that feedback is central to learning and if you do not know how you are doing, you cannot improve. Therefore, this statement applies to all the above mentioned layers (enterprise-wide approach).

Fourth, new practices means new challenges. Organizations will have to continually align and realign, monitor and modify, and search for new ideas so their PM approach will be able to accommodate the new business demands.

Fifth, PM is as described failing organizations all around the world, and obviously it is supported by the top management in the interviewed organizations. Despite the fact that PM is supported by the different C-level executives, we think that in some of the organizations the management lack in their support to a systematic approach to it. From practice, we conclude that the top management often is only interested in approximately 10 KPIs, instead of taking an aggregated enterprise-wide approach in which these 10 indicators are translated to underlying performance measurements. The same as with RM we see a relation between the organization's size and the design and use of PM, as depicted in Figure 13.

Finally, performance indicators are in practice as well as in literature expressed as "KPIs".

8.4 Added Value CA & CM for PM

This research shows that today's environment requires that everyone in an organization is expected to know the organization's strategy to align their activities to support it. Risk and performance management is evolving in the same manner. According to the experts, more and more organizations are incorporating risk and performance at the strategic level, rather than relying on the traditional approach of leaving it to a siloed department. An important factor that contributes to this transformation is technology. Technology like CA & CM tools. In this sub-section we will discuss the added value of CA & CM for PM on the basis of the theoretical and practical findings.

Figure 14 illustrates the ideal theoretical situation in which enterprise-wide risk and performance management are integrated to keep performance and risks in balance, and in which CA & CM tools as technical assets contribute to this process.

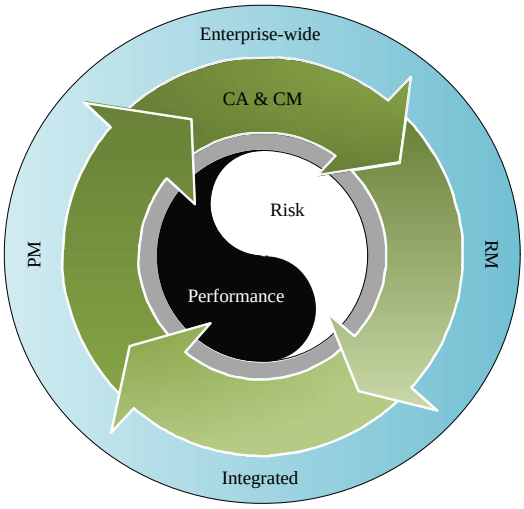

Figure 14: How CA & CM can add value to both, ERM and PM

Unfortunately, this figure by far does not match the current practical situation as illustrated in Figure 15. In practice, the performance and risks management approaches organizations take are not, or to a limited extent, systematically deployed and risk indicators are rarely aligned to the indicators of performance. Recent study underpins this conclusion and shows that many organizations fail to connect risk and performance. Just 37 percent of nearly a hundred senior executives at US-based multinationals surveyed by PwC in 2008 said their organizations link RM to PM [PwC, 2008].

	Organization A	Organization B	Organization C
Employees	+/- 4000	+/- 23000	+/- 2000
Turnover	1 Billion	9 Billion	245 Million
Sector	Civil, Power, and Offshore	Chemical	Public
KCIs address KRIs			
CA & CM add value to RM			
KRIs address KPIs			
RM adds value to PM			
KCIs address KPIs			
CA & CM add value to PM			

Figure 15: Practical Results

As described in previous sub-sections, we determined a positive relation between the size of the organization and its need for a systematic and common RM and PM approach. Furthermore, and more germane to the research contained in this thesis, we anticipate that an integrated approach will be dependent on the proper match between size and sector. The bigger the size, the higher the need for an integrated approach. This relation is depicted in Figure 15.

Each level will have different risk and performance indicators, which makes it a difficult task for organizations to get a reliable view of performance and risks. For example, at the top of the pyramid (e.g., top-management), indicators are expressed in a strategic setting. It will take some analytical and creative effort to aggregate these into new KRIs and KPIs at a lower level (e.g., business unit). I.e., a high level indicator may be expressed in a great variety of indicators at different lower levels. A systematic approach will help organizations and models like the ones from Rouse and Putterill and COSO can assist in this [Rouse and Putterill, 2003, COSO, 2004]. Figure 15 illustrates that in organizations that take a systematic/integrated approach to both: RM and PM, KRIs address KPIs.

As stated above, in establishing an integrated view of risks and performance, every organization will develop its own tailored set of risks and performance indicators. But whatever metrics an organization determines to be most informative, the data underlying those measures must be consistent and reliable across the whole business. This is exactly the most profound added value of CA & CM currently observed in practice, unfortunately only for the secondary processes.

Management strives to look at risk and performance information that reflects the current state of the organization. But the current CA & CM approaches only ensures this consistency and reliability for the secondary processes, instead of ensuring reliability for the primary processes.

However, each organization is different and the audit activity's approach to, and amount of, CA & CM depends on the industry in which an organization operates. For example, in the industries of the three described organizations, the core processes are to a limited extent connected or facilitated by IT. In contradiction, e.g., in the financial industry almost all processes are IT facilitated and there are likely automated controls in place. This decreases the effort it will cost to implement CA & CM, to ultimately monitor controls of the primary and secondary processes on an automated and continuous basis.

Furthermore, if the primary processes are IT facilitated and have automated control in place, CA & CM can provide the management with accurate data and timely reporting of key risk and performance issues. CA & CM tools will alert auditors or management in case of any critical failure or event. Thereby it creates the ability to consider and analyze large volumes of transactions in less time, more automatically, more efficiently, and more cost-effectively than using the more traditional and manual sampling (snapshot) techniques.

Despite the high level of IT facilitated processes and automated controls, there could still be some problems. For example, a problem organizations face is that information resides in too many places across the enterprise. We think that fragmented information is difficult, if not possible, to act on. For example, creating an agile and risk aware PM process is difficult to accomplish if you rely on numerous disconnected spreadsheets that are periodically refreshed by random downloads from numerous different transaction system.

Concluding from this, leading an organization to think about, and act on, risk and performance in an integrated way to which CA & CM contributes as depicted in Figure 14 will face its roadblocks. But by focusing first on a few key areas for integration and improvements, organizations can make great strides toward implementing a fresh approach that meets the challenges of today's world.

Part VI
Conclusions

This is the last part of this research and it provides the reader with conclusions and recommendation. It furthermore answers the main question as described in Section 2.

Contents of Part VI

9 Conclusions & Recommendations

Respectively 38 (significant) and 58 (moderated) percent of the organizations which contributed to the research of KPMG about the status of CA & CM in the Netherlands, see CA & CM as a benefit for process improvement [KPMG, 2010b]. But, only 20 (significant) and 49 (moderated) percent think that CA & CM can contribute to PM. The research outlined in this thesis shows to what extent the 20 + 49 = 69 percent are right. The main question that is answered in this research is:

> *To what extent can Continuous Auditing (CA) & Continuous Monitoring (CM) be of added value for Performance Management (PM)?*

The days of PM based only on detailed, static plans and budgets that offer an accounting view of the business are numbered. Environmental uncertainties, new laws and regulations like SOX, and new technology dictate that organizations develop a set of PM practices that allow managers to identify, understand and manage risks and controls as a continuous part of their management process. But creating an agile and risk aware PM process is difficult to accomplish if organizations are relying on numerous disconnected spreadsheets that are periodically, often manually refreshed with information from numerous different transaction processes. Nevertheless, in today's environment, the combination of best practices from experts and state of the art technology like CA & CM tools can provide managers with the means to turn RM into a key component of their ability to manage an organization's performance.

Conclusions Using CA & CM and ERM, to focus PM not only on performance, but also on risk and control is a critical element of being able to effectively support an organization operating in an uncertain world; and today with the financial crisis, that means all organizations.

From practice we conclude that organizations are narrowly focusing their CA & CM activities on regulatory compliance. A research of KPMG at 138 organizations in the Netherlands revealed that the majority of the enterprises are starting CA & CM initiatives from a compliance perspective instead of taking a broader view about enterprise-wide risk and performance management [KPMG, 2010b]. In this way, not able to achieve all potential benefits of CA & CM for PM:

- The greatest benefit of CA & CM that is currently observed in practice is a sense of reliability of performance and risk information. Management strives to look at risk and performance information that reflects the current state of the organization. With CA & CM, organizations are able to increase the number and frequency of measurements (underlying controls), which ultimately leads to more reliable information.

- Furthermore, CA & CM can provide the management with accurate data and timely reporting of the key risk and performance issues, because such

tooling will automatically alert auditors or management in case of any critical failure or event.

- In addition, it creates the ability to consider and analyze large volumes of transactions in less time, more automatically, more efficiently, and ultimately more cost-effectively than using the traditional and manual sampling (snapshot) techniques.

Recommendations To reach these potential benefits, organizations should understand the extent to what they have to transform their performance and risk management approaches, controls, infrastructure, technology, and people before they start implementing. The extent of the benefits described above are depending on several factors. The organizations in this research should take some critical steps to achieve these potential benefits:

- First, when an organization wants to achieve the maximum benefit out of their CA & CM activities, it is essential that RM and PM are applied in a strategy setting and across the entire organization. In an ideal situation, they are integrated as described in the previous section. In practice we determined a positive relation between the organization's size and the design and use of an integrated approach to RM and PM. Nevertheless, only one of the three organizations takes such integrated approach.
- Second, in Part II we elaborated on frameworks that could help organizations to take such enterprise-wide and strategic approaches to RM and PM. Again, there is a gap between the described theory and the current practical situation. Only one of the three organizations described in this research uses a common RM framework, and not one is using a common PM framework.
- Third, after they have set up their enterprise-wide/integrated PM and RM, organizations should investigate and decide if CA & CM can contribute to these processes. This decision could be based on several factors. We will briefly mention the most important ones:
  - Depending on the organization's industry and core risks, primary and/or secondary processes should be IT-facilitated. In two of the three interviewed organizations, only the secondary processes (e.g., order-to-cash and procure-to-pay) are facilitated by IT, while the primary processes are to a limited extent, or not at all facilitated by IT.
  - A minimum of 60 to 70 percent of the controls should be automated. Obviously, organizations will always have some level of manual controls, but unfortunately in practice more than likely of the control are manual. The key is to balance between a combination of automated and manual controls, because opportunities exist to create value from both.

- CA & CM can be most beneficial when primary and secondary processes are standardized and facilitated by common IT systems, data and infrastructure. From practice we conclude that in this way, organizations are more likely to succeed in leveraging their investment in CA & CM across the entire organization.
- CA & CM activities should furthermore be centralized, thereby enabling that systems can be centrally monitored. Conversely, organizations that have a wide variety of processes, systems, data and infrastructure may have to adapt or customize their CA & CM approach every time. They even may deploy different tools for different environments. In such environment, it will be less beneficial to implement CA & CM. More and more organizations are centralizing their IT systems. Nevertheless, in practice still a lot of organizations do have a decentralized structure.
- Responsibilities will shift with the introduction of CA & CM. Interviews with experts of KPMG revealed that internal auditors within the next five years will experience a shift in their role/activities from providing information to providing interpretation. They should offer, and may even are expected to offer, increased synthesis and analysis of performance and risk information to help the management identify business exceptions and challenges. This will require the auditors to create a broader understanding of the organization and thereby, of its core processes, systems, objectives and risks.

Final Conclusion Creating value with CA & CM for PM is an opportunity in the sense that it makes it possible to sell CA & CM as a profit driver. An integrated approach to manage risk and performance with the help of CA & CM is about using the right information to achieve an up-to-date meaningful view of risk across the enterprise and to more accurately anticipate the associated impact on performance, layering that information into strategy setting and decision making. But in spite of all that, organizations should create an environment in which CA & CM can reach its full potential, and this is exactly where organizations should achieve some major improvements. There is potential for CA & CM to add value to PM, but organizations have a long way to go!

10 Further Research

We believe this research provides an initial foundation that can spawn additional research on CA & CM, RM and PM. Yet, there are still some interesting fields to explore which can improve this research.

First, further research can improve the model as depicted in Figure 9 at the beginning of Section 6. Further research about new CA & CM, RM and PM technologies will give insight in the completeness of the model. Technology is growing and will more and more be used in organizations to manage performance and risks. Therefore, it is interesting to investigate the completeness of the model in about 5 years from writing this thesis.

Second, it will be very interesting to validate the theoretical findings on the basis of significantly more interviews with experts. Due to a lack of time, we interviewed employees of three different organizations in the Netherlands and three experts of KPMG on the field of CA & CM, RM and PM, but to test the validity of the findings, this number should be extended.

Third, further research is needed before it is possible to trust on the findings. Case studies and maybe some pilots can be conducted. This will highlight the best practices and may result in a business case and implementation plan.

Finally, it could also be interesting to explore and test the different tools and methods used for CA & CM and PM. In this research a few tools are described, but not tested on the extent to what they can be of added value to RM and PM. Furthermore, we only discussed the COSO ERM - Integrated Framework and the Integral Framework for Performance Measurement in this research [COSO, 2004, Rouse and Putterill, 2003], but researchers may investigate which other frameworks are interesting, like the COBIT framework [The COBIT Steering Committee and the IT Governance Institute, 2000].

This research provides KPMG with a first impression about the extent to what CA & CM can be of added value for PM, but does not goes into detail about which different tools, methodologies, frameworks, businesses, and processes that can be most beneficial for PM.

References

ACL Services Ltd. Control Assurance for the Order-to-Cash Cycle: Support Regulatory Compliance, Gain Insight, Improve Revenue Recovery. *ACL Services Ltd., Printed in Canada*, 2005.

ACL Services Ltd. Control Assurance for Payroll: Drive Operational Performance, Control Costs, Support Regulatory Compliance. *ACL Services Ltd., Printed in Canada*, 2006.

M. Alles, Brennan G., Kogan A., and Vasarhelyi M.A. 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, 2006a. ISSN 1467-0895. doi: DOI: 10.1016/j.accinf.2005.10.004. 2005 Research Symposium on Integrity, Privacy, Security & Trust in an IT Context.

M. Alles, F. Tostes, M. Vasarhelyi, and E.L. Riccio. Continuous Auditing: the USA Experience and Considerations for its Implementation in Brazil. *Revista de Gesto da Tecnologia e Sistemas de Informao*, 3(2):211–224, 2006b.

M.G. Alles, A. Kogan, and M.A. Vasarhelyi. Putting Continuous Auditing Theory Into Practice: Lessons from Two Pilot Implementations. *Journal of Information Systems*, pages 195–214, 2008.

M. Beasley, A Chen, N. Nunez, and L. Wright. Working Hand in Hand: Balanced Scorecards and Enterprise Risk Management. *Strategic Finance*, 2006.

J.L. Bierstaker, P. Burnaby, and J. Thibodeau. The Impact of Information Technology on the Audit Process: an Assessment of the State of the Art and Implications for the Future. *Managerial Auditing Journal*, pages 64–159, 2001.

P.V. Boccasam. Approva Automates Audit Processes for Greater Compliance and Efficiency. *Approva Corporation*, 2010.

D.M. Bowling and L.A. Rieger. Making Sense of COSO's New Framework for Enterprise Risk Management. *Bank Accounting & Finance*, pages 35–40, 2005.

D.V. Broady and H.A. Roland. *Titel SAP GRC For Dummies.* For Dummies, 2008.

BWise. BWise, Business in Control. http://www.bwise.com/solutions-services/solution-components, December 2010.

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

D. Coderre. Recommendations for an Effective Continuous Audit Process. *Internal Audit*, 17:1–7, 2007.

D. Coderre. Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment. *Global Technology Audit Guide*, 2008.

G. Cokins and P. Mestchian. Risk-Based Performance Management - Making it Work. *Journal of Risk Intelligence*, pages 25–28, 2006.

T.J. Cook, J. Vansant, L. Stewart, and J. Adrian. Performance Measurement: Lessons Learned for Development Management. *World Development*, 23(8): 1303–1315, 1995. ISSN 0305-750X. doi: DOI: 10.1016/0305-750X(95)00050-M.

R. Cooper and R.S. Kaplan. Profit Priorities from Activity-Based Costing. *Harvard Business Review*, 69:130–135, 1997.

COSO. Internal Control - Integrated Framework: Executive Summary. *Committee of Sponsoring Organizations of the Treadway Commission*, 1994.

COSO. Enterprise Risk Management - Integrated Framework: Executive Summary. *Committee of Sponsoring Organizations of the Treadway Commission*, 2004.

COSO. Internal Control - Integrated Framework: Guidance on Monitoring Internal Control Systems. *Committee of Sponsoring Organizations of the Treadway Commission*, 2009.

S. Datar and M.G. Alles. How Do you Stop the Books from Being Cooked? A Management Control Perspective on Financial Accounting Standard Setting and the Section 404 Requirement of the Sarbanes/Oxley Act. *International Journal of Disclosure & Governance*, 1(2):119–137, 2006.

I.E. Davies. Evaluation and Performance Management in Government. *SAGE Publications, London, Thousand Oaks and New Delhi*, 1999.

A. de Jong, D.V. de Jong, G.M.H. Mertens, and P.G.J. Roosenboom. Royal Ahold: A Failure of Corporate Governance and an Accounting Scandal. *Tilburg University, Center for Economic Research*, 2005.

M. de Schiffart. Op Zoek Naar het Risico 'Ijsbeer'. *Financieel Management*, 2010.

Deloitte Development LCC. Continuous Monitoring and Continuous Auditing: From Idea to Implementation. 2010.

M. Drew. Information Risk Management and Compliance Expect the Unexpected. *BT Technology Journal*, 25(1):19–29, 2007. doi: DOI: 10.1007/s10550-007-0004-x.

R.G. Eccles. The Performance Measurement Manifesto. *Harvard Business Review*, pages 131–137, 1991.

Ernst & Young. A New Balanced ScoreCard: Measuring Performance and Risk. *EYGM Limited*, 2009.

Ernst & Young. Risk Appetite: The Strategic Balancing Act. *EYGM Limited*, 2010.

S. Flowerday and R. von Solms. Continuous Auditing: Verifying Information Integrity and Providing Assurances for Financial Reports. *Computer Fraud & Security*, 2005(7):12 – 16, 2005. ISSN 1361-3723. doi: DOI: 10.1016/S1361-3723(05)70232-3.

S. Flowerday, A.W. Blundell, and R. Von Solms. Continuous Auditing Technologies and Models: A Discussion. *Computers & Security*, 25(5):325–331, 2006. ISSN 0167-4048. doi: DOI: 10.1016/j.cose.2006.06.004.

D. Forsythe. *Quicker, Better, Cheaper? Performance Management in American Government*. Rockefeller Institute Press, Albany, NY, 2001.

General Counsel Roundtable. Seizing the Opportunity, Part One: Benchmarking Compliance Programs. *http://www.generalcounselroundtable.com*, 2003.

C. Harland, R. Brenchley, and H. Walker. Risk in Supply Networks. *Journal of Purchasing and Supply Management*, 9(2):51 – 62, 2003. ISSN 1478–4092. doi: DOI: 10.1016/S1478-4092(03)00004-9. Supply Chain Management: Selected Papers from the European Operations Management Association 8th International Annual Conference.

E.M Heffes. Theory to Practice: Continuous Auditing Gains. *Financial Executive*, pages 17–18, 2006.

F. Ibrahim and D. Hallemeesch. Het Effect van GRC-software op de Jaarrekeningcontrole. *Compact*, 2008.

K. Jagan, R. Dasaratha, and Z. Yinghong. Costs to Comply with SOX Section 404. *Auditing: A Journal of Practice & Theory*, 27(1):169–186, 2008.

C.C. Johnson and I. Beiman. Balanced Scorecard for State-Owned Enterprises. *Asian Development Bank*, 2007.

R.S. Kaplan and D.P. Norton. Using the Balanced Scorecard as a Strategic Management System. *Harvard Business Review*, pages 1–13, 1996a.

R.S. Kaplan and D.P. Norton. *De Balanced Scorecard: Translating Strategy into Action*. Harvard Business School Publishing Corporation, 1996b.

S. Kemper. *A Story of Genius, Innovation, and Grand Ambition*. HarperCollins Publishers, 2005.

A. Kogan, E.F. Sudit, and M.A. Vasarhelyi. Continuous Online Auditing: An Evolution. *Journal of Information Systems*, 2010.

Koninklijke Ahold, N.V. Ahold, Make it Easy to Choose the Best. http://www.ahold.com, December 2010.

T. Kothari and D.R. Fesenmaier. Performance Measurement and Performance Management. *In Proceedings of the 11th Annual Graduate Education and Graduate Student Research Conference in Hospitality and Tourism*, 2006.

KPMG. Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance. 2009.

KPMG. Continuous Auditing and Monitoring: Are Promised Benefits Now Being Realised? 2010a.

KPMG. De Status van CA & CM Binnen Nederlandse Organisaties. 2010b.

KPMG International Cooperative. KPMG, Cutting Through Complexity. http://www.kpmg.com/global/en/Pages/default.aspx, December 2010.

R.J. Kuhn and S.G. Sutton. Learning from WorldCom: Implications for Fraud Detection through Continuous Assurance. *Journal of Emerging Technologies in Accounting*, 3(1):61–80, 2006. doi: 10.2308/jeta.2006.3.1.61.

M. Lebas and K. Euske. *Business Performance Management: Theory and Practice*. Cambridge University Press, 2002.

M.J. Lebas. Performance Measurement and Performance Management. *International Journal of Production Economics*, 1995.

S.H. Li, S.M. Huang, and Y.C.G. Lin. Developing a Continuous Auditing Assistance System Based on Information Process Models. *Journal of Computer Information Systems*, 2007.

P. Lichiello. *Turning Point Guidebook for Performance Measurement*. Turning Point National Program Office at the University of Washington, 1999.

J.H. Lingle and W.A. Schieman. From Balanced Scorecard to Strategic Gauges: is Measurement Worth It? *Management Review*, 85, 1996.

C. McKittrick. Identify 'Surprises' Before It's Too Late. *The McKittrick Report*, 2009.

R.R. Moeller. *COSO Enterprise Risk Management: Understanding the new Integrated ERM Framework*. John Wiley & Sons, Inc., 2007.

U.W. Nabitz and N.S. Klazinga. EFQM approach and the Dutch Quality Award. *International Journal of Health Care Quality Assurance*, 12(2):65–71, 1999.

National Partnership for Reinventing Government. *Serving the American Public: Best Practices in Performance Measurement*. United States Government Printing Office, 1997.

A. Neely. The Performance Measurement Revolution: Why Now and What Next? *International Journal of Operations & Production Management*, 19 (2):205–228, 1999.

A. Neely, C. Adams, and M. Kennerly. *The Performance Prism: The Scorecard for Measuring and Managing Success*. Financial Times Prentice-Hall, 2002.

O. Neyran and B. Nizamettin. Measuring Business Performance in the Context of the Turkish Manufacturing Industry. *Istanbul University*, 2007.

M.J. Nigrini and A.J. Johnson. Using Key Performance Indicators and Risk Measures in Continuous Monitoring. *Journal of Emerging Technologies in Accounting*, pages 65–80, 2008.

P.R. Niven. *Balanced Scorecard Step-By-Step: Maximizing Performance and Maintaining Results*. John Wiley & Sons, Inc., 2006.

Oracle Corporation. Information Governs: Run Your Organization Better- and Prove It. *Oracle Solutions for Governance, Risk, and Compliance*, 2008.

Oracle Corporation. Uncertainty Management: Risk and Performance, Two Sides of the Same Coin. *Oracle Solutions for Governance, Risk, and Compliance*, 2009.

D. Otley. Performance Management: a Framework for Management Control Systems Research. *Management Accounting Research*, 10(4):363 – 382, 1999. ISSN 1044-5005. doi: DOI: 10.1006/mare.1999.0115.

D. Parmenter. *Key Performance Indicators (KPI): Developing, Implementing, and Using Winning KPIs*. John Wiley & Sons, Inc., 2 edition, 2010. ISBN 978-0-470-54515-7.

PwC. Managing Business Performance: The Metrics that Matter. 2008.

R.E. Quinn and J. Rohrbaugh. A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis. *Management Science*, 29:363–377, 1983.

Z. Rezaee, A. Sharbatoghlie, and R. Elam. Continuous Auditing: Building Automated Auditing Capability. *Auditing: A Journal of Practice & Theory*, 21(1):147–163, March 2002.

W.P. Rogerson. Intertemporal Cost Allocation and Managerial Investment Incentives: A Theory Explaining the Use of Economic Value Added as a Performance Measure. *The Journal of Political Economy*, 105(4):770–795, 1997.

P. Rouse and M. Putterill. An Integral Framework for Performance Measurement. *Management Decision*, pages 791–805, 2003.

G. Rumble. *The Costs and Economics of Open and Distance Learning*. Kogan Page, 1997.

G.A. Rummler and A.P. Brache. *Improving Performance: How To Manage the White Space on the Organization Chart. Second Edition. The Jossey-Bass Management Series.* Jossey-Bass, Inc., 350 Sansome Street, San Francisco, CA 94104, 1995.

D. Searcy, J. Woodroof, and B. Behn. Continuous Audit: The Motivations, Benefits, Problems, and Challenges Identified by Partners of a Big 4 Accounting Firm. *Hawaii International Conference on System Sciences*, 7:210, 2003. doi: http://doi.ieeecomputersociety.org/10.1109/HICSS.2003.1174565.

S.J. Shaw. *Corporate Governance & Risk*. John Wiley & Sons, 2003.

D.S. Sink. The Role of Measurement in Achieving World Class Quality and Productivity Management. *Industrial Engineering*, 2007.

The COBIT Steering Committee and the IT Governance Institute. COBIT Framework, 3rd Edition. *Information Systems Audit and Control Foundation*, 2000.

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

N. Venkatraman and V. Ramanujam. Measurement of Business Performance in Strategy Research: A Comparison of Approaches. *The Academy of Management Review*, 11(4):801–814, 1986.

P. Verschuren and H. Doorewaard. *Designing a Research Project*. LEMNA, 2005.

J.D. Wisner and S.E. Fawcett. Link Firm Strategy to Operating Decisions Through Performance Measurement. *Production and Inventory Management Journal*, pages 5–1, 1991.

Part VII
Appendices

This part provides background information for readers who like to know more details about the research. The content throughout this thesis refers to this Appendix, where the reader can find additional information regarding this research.

Contents of Part VII

A CA & CM Tools

A number of tools are available for CA & CM. Tools can range from spreadsheet software or scripts, to commercial packaged solutions or custom-developed systems. The right choice will depend on the organization's business requirements and the desired benefits, including practical considerations such as how well the proposed tool will integrate with existing systems.

Generally CA & CM tools fall into two categories: those that are integrated within ERP applications, such as SAP GRC, and Oracle GRC; and specialized add-on tools such as Approva, ACL, BWise, Xactions, and SynAxion. Almost all of these applications offer one or both of two fundamental monitoring capabilities: user authorizations/segregation of duties and monitoring process/transaction controls. The following sub-sections briefly describe the tools.

A.1 SAP GRC

SAP delivers an integrated portfolio of Governance, Risk, and Compliance applications: SAP GRC. It offers a full range of functionality to ensure that financial information is accurate, risks are being managed, regulations are being complied with, and that the probability of nasty surprises is as low as it can be [Broady and Roland, 2008]. It is a comprehensive solution, fully integrated in an organization's existing SAP, Oracle, PeopleSoft or other Legacy system; or as a stand-alone solution, it manages the user access, controls and monitors of business operations and actively warns auditors or management in case of possible or potential thefts, frauds or other critical risks to an organization's business. The architecture model of SAP GRC is depicted in Figure 16.

In Figure 16 you can see that the SAP GRC solutions addresses four compliance and control processes. We see these four processes as main CA & CM activities in the SAP GRC solution. Therefore, the next four paragraphs elaborate on these.

Access Control With this module, organizations will save significant effort and reduce risks when creating, maintaining and retiring users, and automatically assign correct authorization in all related systems. The integrated work flow assures approval by respective business line managers and an fully automated risk analysis will alert auditors or management in case of any critical combination of authorizations assigned to the user.

Process Control An organization's ongoing, operational business processes and transactions will be monitored by the process control module. This checks for every business transaction if any rule defined is being violated, if any potential risk of theft or fraud occurs, and will pro actively warn auditors or management in case of any problems or risks. Furthermore, all activities and incidents are documented and can be audited at any time. This module also en-

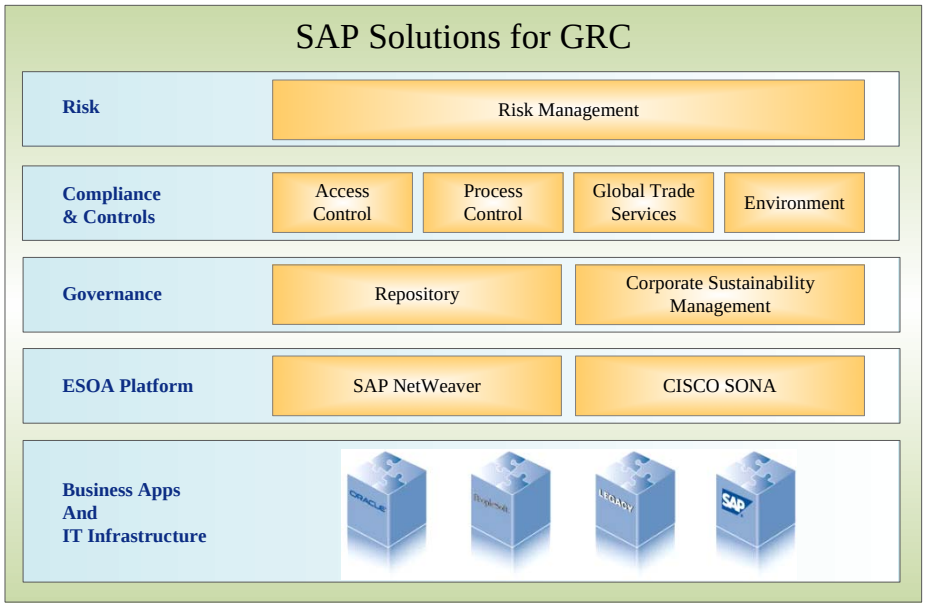

Figure 16: Architecture model SAP Solutions for GRC.

sures full compliance with international standards and requirements, like SOX and Basel II.

Global Trade Services This module ensures an organization's compliance in terms of international customs regulations, consisting of export management, import management, trade preferences management and restitution management. The module can receive data from SAP, Oracle or any other ERP system and includes monitoring of sanctioned party lists: US-ITAR, EU-REACH, NAFTA preferences (legislations), nested licenses, duty calculations and fully automated customs declarations based on transactions in an organization's ERP systems.

Environmental SAP Environment, is the SAP solution for supporting an organization's Environment Health & Safety EHS management processes. It supports dealing with rules and regulations and ensures organization's compliance with these rules and regulations. It provides the tools to automate the checks and administration in an organization's logistical and product stewardship processes, thus securing that an organization operate in a compliant, efficient and secure way. SAP EHS is regularly updated with new functionality prompted by new regulations.

These processes are via an Enterprise Service Oriented Architecture (ESOA) with tools like SAP NetWeaver and CISCO SONA, be fully integrated in an

organization's existing SAP, Oracle, PeopleSoft or other Legacy system, as illustrated in Figure 16.

A.2 Oracle GRC Solutions

Oracle GRC is designed to work on an integrated basis within the Oracle stable of products. It operates from an application server attached to the target ERP system, monitoring data at source. Reporting is through email alerts or dashboards [Oracle Corporation, 2008]. It is designed to integrate with Oracle Applications (EBS, PeopleSoft, JDE, Siebel) as well as other non-Oracle ERP solutions (such as SAP, Lawson, etc.). As depicted in Figure 17, is it comprised of the following modules: GRC Intelligence, GRC Manager, and GRC Controls Management.

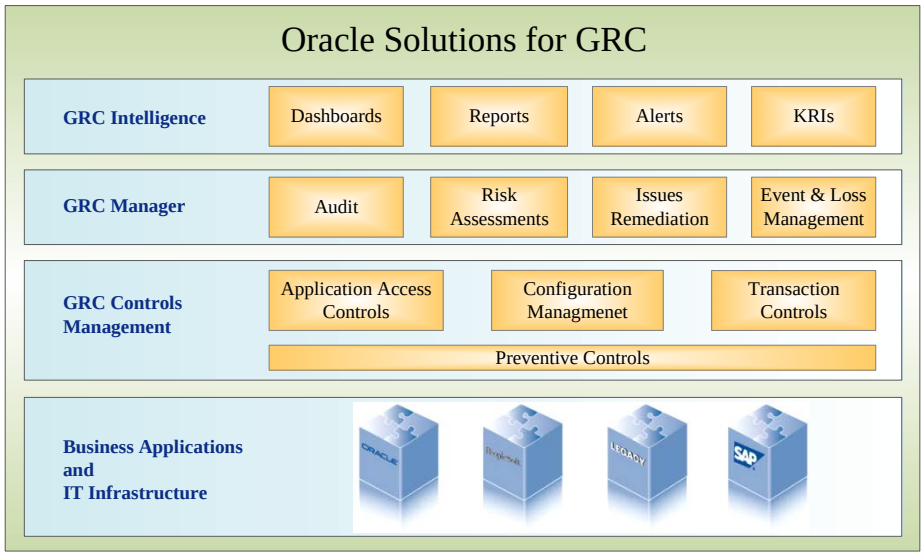

Figure 17: Architecture model Oracle Solutions for GRC.

We see the four processes of GRC Controls Management as the main CA & CM activities in the Oracle GRC solution. The four modules are presented in the following four paragraphs.

Configuration Controls This module controls and tracks changes to critical functional configurations or application setups, using approval work flows and notifications to facilitate change management without negatively impacting core business operations. With this module, organizations can ensure application integrity and audit changes, and continuously monitor setups and code [Oracle Corporation, 2008].

Application Access Controls This one provides real-time monitoring and proactive enforcement of crucial access policies, such as Segregation of Duties (SoD). The system anticipates potential SoD conflicts before they arise and makes it easy to grant appropriate application access and reduce risk across an organization's user base. Oracle application access controls can also extents key access controls to temporary users [Oracle Corporation, 2008].

Transaction Controls The third module continuously monitors transactions against policies to detect suspicious business practices or explicit control violations. The system pro actively alerts stakeholders of events for effective and timely remediation of violations. Oracle transaction controls provides controls that encompass business processes such as purchasing, inventory, receivables, and revenue recognition, and general computer controls that track system access and user activation status [Oracle Corporation, 2008].

Preventive Controls Finally, this module works with the other modules within the Oracle GRC controls suite to prevent unauthorized changes to critical application data and setups and enforce real-time policy changes at a granular application level. Oracle preventive controls offers simulation of SoD scenarios as well as monitoring and prevention of unauthorized changes to critical data [Oracle Corporation, 2008].

A.3 BWise

BWise offers a GRC management platform composed of several components. All components are an integrated part of the GRC platform. The GRC platform is depicted in Figure 18.

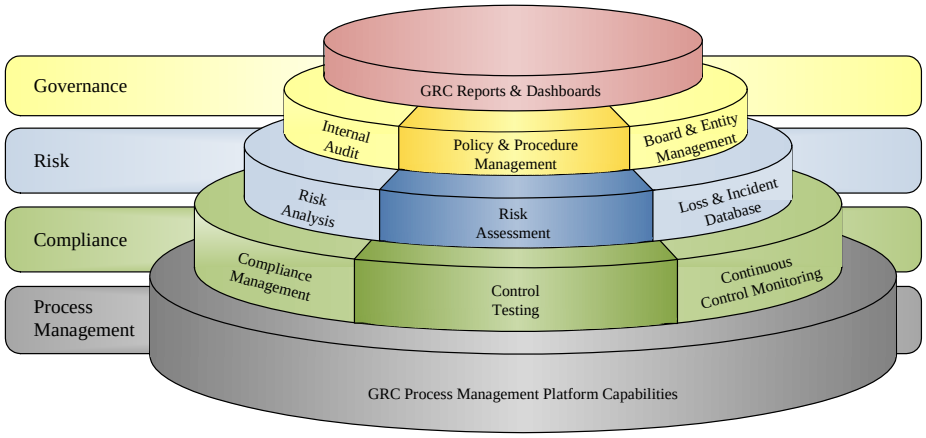

Figure 18: Architecture model BWise GRC.

Organizations can implement individual solution components to meet their specific GRC needs or implement the entire GRC platform.

The BWise GRC platform consists of four layers, a governance layer, a risk layer, a compliance layer and a process management layer. Each layer is divided into three components that have the required capabilities to fully embed GRC and process management into an organization. The BWise GRC platform also enables companies to prove to external parties, such as external accountants or consultants, or government regulators that it is in control of its internal controls and risks [BWise, 2010].

Process management is the basic layer that enables an organization to truly integrate its individual GRC processes, and to drive efficiencies based on the reduction of key controls and audit costs. An effective GRC system, based on process management, enables a company to have more secure control over growth activities, as an example enabling subsidiary establishment in a matter of weeks. On a day to day basis, process management will present how processes are performing and where improvements are required. This ultimately enables an increase in business performance.

According to BWise, CA & CM are at the forefront of business process performance and on the mind of any business manager who wants to be in control [BWise, 2010]. CA & CM provide the necessary assurance that processes, systems and operational KPIs or KRIs are running in compliance. The continuous control monitoring component, located at the second layer of the platform depicted in Figure 18 is the core CA & CM component of BWise.

It can integrate with any system or database to manage and monitor key quantitative risks, including systems such as SAP, Oracle, financial systems and IT management systems. “Management by exception” initiatives can now be fully integrated into the enterprise’s GRC and risk management by keeping track of key risks. It furthermore includes standard rules, and beside that allows organizations to fine tune rules and create new rules. It can also collect auditable evidence from external systems. And as depicted in Figure 18, it seamlessly integrates with the BWise GRC platform, managing an organization’s risks and ensuring that they are in control.

A.4 Approva

Approva designed their tool to monitor automated controls for key financial applications such as SAP, Oracle, and PeopleSoft. Approva allows IT departments to push the management of controls to the business users who are ultimately accountable for them. Boccasam says this is a key to compliance, and should be the first consideration in evaluating continuous controls monitoring solutions [Boccasam, 2010]. Approva is a CA & CM solutions with out-of-the-box content that monitors and correlates four control types for multiple applications and business processes as illustrated in Figure 19.

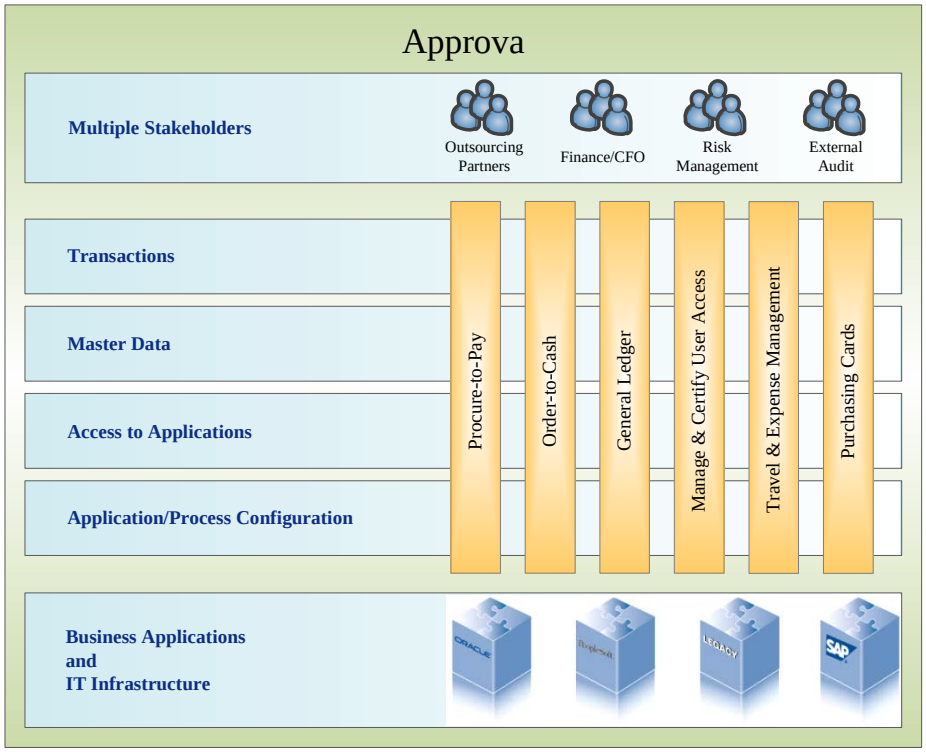

Figure 19: Architecture model Approva.

A.5 ACL CCM

CCM is an add-on for the ACL data analysis tool. It simply comprises a series of standard tests that can be run against transactions data on a daily basis, with the results displayed on a dashboard [ACL Services Ltd., 2005]. CCM have been designed to support the COSO (Committee of Sponsoring Organizations) framework, recognized as the internal controls standard for SOX section 404 compliance [ACL Services Ltd., 2006].

The ACL CCM product suite addresses the following core business processes: Payroll, Purchase-to-Pay Cycle, Travel & Entertainment Expenses, Purchasing Cards, Order-to-Cash Cycle, and General Ledger [ACL Services Ltd., 2005].

The ACL architecture framework is depicted in Figure 20.

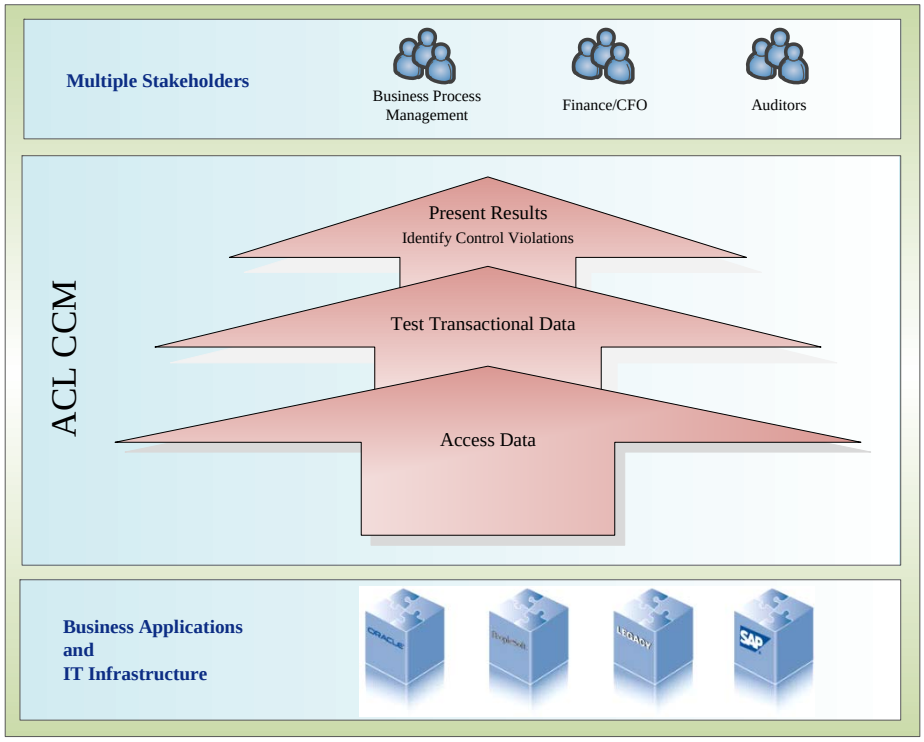

Figure 20: Architecture model ACL CCM, from [ACL Services Ltd., 2005, 2006].

According to ACL, the tool provides visibility into controls health to all stakeholders. The access data vector in the figure presents the review of transactions across all systems and platforms. According to ACL, the tool can review 100 percent of the transactions. The test transactional data vector applies automated tests to critical control points. Finally, the top vector presents quantified control exceptions as an outcome of the other two vectors. In this way the stakeholders will be provided with visibility into control health [ACL Services Ltd., 2006].

A.6 SynAxion

SynAxion provides organizations with a CA & CM software solution that allows them to monitor and optimize quickly, easily and automatically their critical internal controls. SynAxion is implemented at some customers of KPMG. Those organizations can choose four different modules, which can be used for the different processes. In Table 1, the four modules are presented in the left column, four example processes in the top row, and example controls per process in the other cells.

Control	**Purchase to Pay**	**Order to Cash**	**Finance to Report**	**Material to Product**
User controls	Monitoring open invoices	Monitoring open sales orders	Detecting duplicate payments	Detecting dead stock
Configuration controls	3-way match Matching	Configuration of sales condition types	Open posting periods	Configuration for negative stock
Procedural controls	Purchase order request procedure	Discount procedure	Group accounting manual	Scrapping procedure
Authorization controls	Authorization for changing approved purchase orders	Authorization on sales order documents type	Authorization for reversing documents	Authorization for maintaining materials

Table 1: SynAxion CA & CM Controls

KRIs are presented in a scorecard structure. Within this structure, the results are presented by period, business cycle and department. Using these periodic results, the efficiency and effectiveness of controls in the business cycles can be assessed and optimized if necessary. The scorecards results are displayed on key risks like:

- too long outstanding sales orders and purchase orders;
- too long outstanding entries on suspense accounts;
- long lead times in handling of purchase and sales cycles;
- the incorrect use of payments periods, discounts and credit invoices.

SynAxion also includes a data analysis module with the functionalities to detect specific undesired postings or master data. Using predefined filters, it is possible to detect fraudulent activities, incomplete master data, retrospective postings and actual breaches of segregation of duties.

Furthermore the tool can monitor Segregation of Duties (SoD). Important authorization controls to ensure that proper SoDs are reported at various levels:

- monitoring of undesired combinations of authorizations that are granted to a single user;
- monitoring of the actual use of combinations of critical authorizations.

An example of the SynAxion dashboard is depicted in Figure 21.

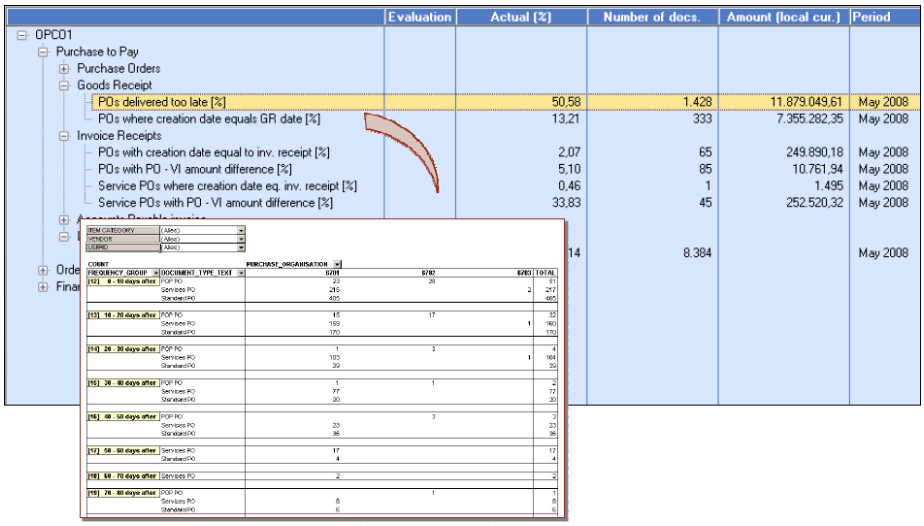

Figure 21: SynAxion dashboard example.

A.7 Xalerts

Xalerts is an enterprise alert & notification product which, unlike many CA & CM products, provides a functional way to alert the stakeholders by sending simple email alerts & notifications. Xalerts leads the field with its device independent mechanism for 2-way multi-channel messaging. The Xalerts architecture is depicted in Figure 22.

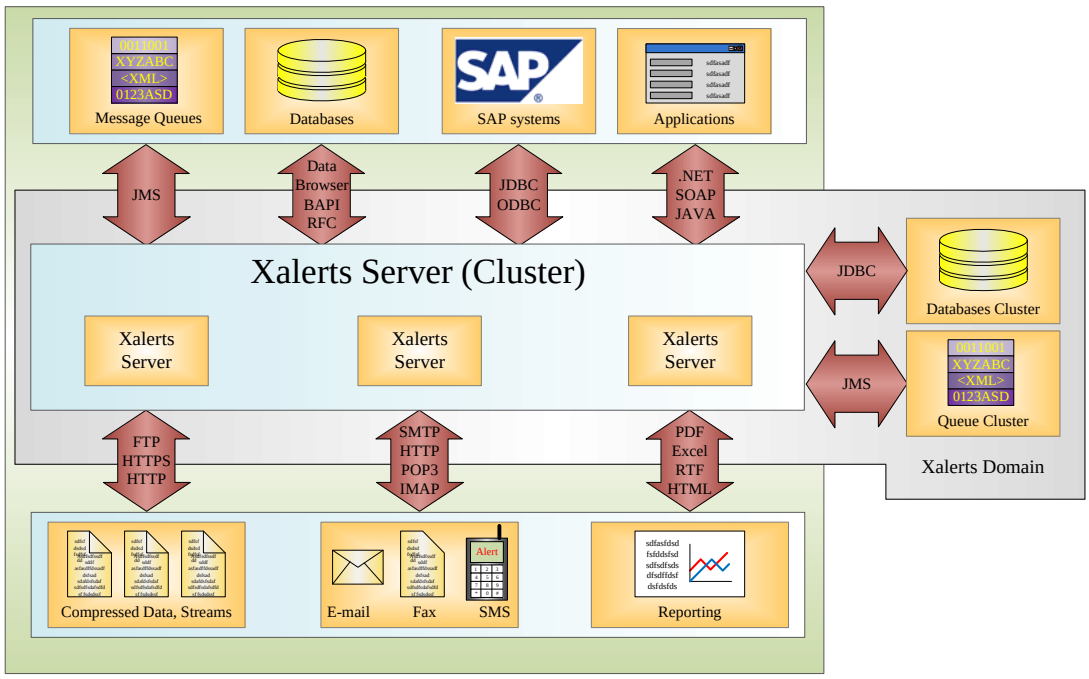

Figure 22: Architecture model Xalerts.

Businesses often have lots of applications and data systems. Xalerts can extract information from almost any system you can imagine, including SAP, J2EE apps, Databases, and Web Services. Stakeholders can be notified by several message standards like e-mail, fax, and mobile text message (SMS).

When organizations switch on to Enterprise Messaging Bus (EMB) and/or Service Oriented Architecture (SOA), often they start to see high volumes of digital business events being created. Xalerts can listen for these events, usually in XML format, and provide intelligent decision making and work flow functionality based on the content of these messages. Furthermore as depicted in Figure 22, Xalerts has also support for other standards including: SMTP, POP3, IMAP, HTTP, HTTPS, SNMP, XPATH, JavaScript, FTP, JMS, PGP, SQL, JDBC, S/MIME, SMS, WAP.

B PM Methodologies

B.1 Activity Based Costing (ABC)

ABC is a method of analyzing business operations that leads to cost identifications (e.g., direct costs and indirect costs) and cost classifications based on activities [Kothari and Fesenmaier, 2006]. It is generally used as a tool for understanding product and customer cost and profitability [Cooper and Kaplan, 1997, Johnson and Beiman, 2007]. As such, ABC has predominantly been used to support strategic decisions such as pricing, outsourcing, identification and measurement of process improvement initiatives [Cooper and Kaplan, 1997]. The central assumption of the ABC approach is illustrated in Figure 23.

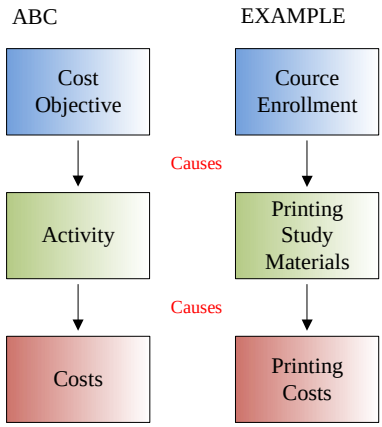

Figure 23: Activity Based Costing (ABC), from [Rumble, 1997].

In the ABC depicted in Figure 23, cost objects are the reasons for carrying out activities and may include products, services or customers. An activity is defined as any process or procedure that causes work to be done. Related activities are frequently clustered by function or process into an activity center. As any productive activity requires labor, materials and equipment, it will incur certain costs.

While organizations will likely benefit from ABC, it is mainly an accounting and cost-based method of viewing and analyzing an organization and its acuities [Johnson and Beiman, 2007]. This could be a reason why ABC lost ground in the 1990s, to alternative metrics, such as the Economic Value Added (EVA) [Kaplan and Norton, 1996b].

B.2 Economic Value Added (EVA)

EVA is most directly linked to the creation of shareholder value [Otley, 1999]. To calculate EVA, organizations need accounting figures from the balance sheet and the income statement. The EVA represents the organizations profit after

full cost of capital [Rogerson, 1997]. There are four steps in the calculation of EVA:

1. calculate Net Operating Profit After Tax (NOPAT);
2. calculate Total Invested Capital (TC);
3. determine the Weighted Average Cost of Capital (WACC);
4. calculate EVA = (NOPAT - WACC%) * TC.

Developed by the management consulting firm Stern Stewart, EVA really caught fire in the 1990s. Big corporations, including Coca-Cola, General Motors, and AT&T, employ EVA internally to measure performance [Rogerson, 1997]. Despite the adoption in big corporations, EVA is particularly difficult to calculate and prone to errors that can lead to misleading results [Johnson and Beiman, 2007]. Furthermore, if organizations are publicly traded, they better tend to avoid EVA as PM tool due to its complexity [Johnson and Beiman, 2007].

B.3 Balanced ScoreCard (BSC)

Developed by Kaplan and Norton [Kaplan and Norton, 1996a] in the 1990s and partly based on the Competing Values Framework of Quinn and Rohrbaugh [Quinn and Rohrbaugh, 1983], the BSC have found a widespread adoption in varied industries, and is one of the most widely used PM tools in the world [Lebas, 1995, Lebas and Euske, 2002, Beasley et al., 2006, Johnson and Beiman, 2007]. For this reason we will elaborate in more detail on the BSC in comparison with other PM tools.

The BSC integrates four sets of measurements, complementing traditional financial measures with those driving future performance. The BSC is illustrated in Figure 24.

Kaplan and Norton describe the origin of the name: “the name Balanced ScoreCard reflects the balance provided between short- and long-term objectives, between financial- and non-financial targets, between lagging and leading KPIs, and between external and internal performance perspectives“ [Kaplan and Norton, 1996b]. We will elaborate on the perspectives in the next four paragraphs.

Financial perspective The financial perspective provides a view of how the shareholders see the organization. By including this perspective it shows that Kaplan and Norton have not turned away from the need for financial data, but instead have incorporated it into a measurement and strategy model that includes a more holistic view of the organization’s business strategies [Kaplan and Norton, 1996a].

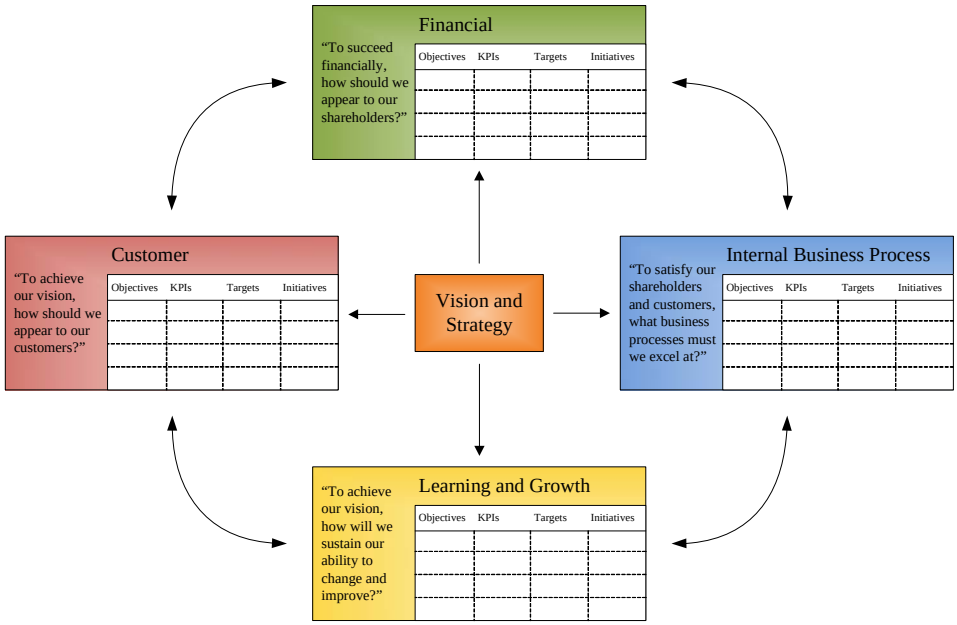

Figure 24: Balanced ScoreCard (BSC), from [Kaplan and Norton, 1996a].

Customer perspective This perspective provides a view of how the customers see the organization. Kaplan and Norton contend that, "to put the balanced scorecard to work, companies should articulate goals for time, quality, performance, and service; and then translate these goals into specific measures" [Kaplan and Norton, 1996a]. Overall, this is a measure of how the organization provides value to the customer. For example, it is not enough to simply bring down the cost of an item. The delivery time and manner in which the customer is dealt during times of sales and support are important as well.

Internal business process perspective The internal business process perspective provides a view of what the organization must excel at to be competitive. The focus of this perspective, is the translation of customer-based measures into measures reflecting the organization's internal operations [Kaplan and Norton, 1996a]. The highest level in this measurable should be on customer satisfaction and factors affecting such issues as cycle time, quality, employee skills, and productivity. Kaplan and Norton recommend that, "companies also attempt to identify and measure their organization's core competencies, the critical technologies needed to ensure continued market leadership" [Kaplan and Norton, 1996a].

Learning and growth perspective Kaplan and Norton underscore the importance of innovation and growth in their statement that, "an organization's ability to innovate, improve, and learn ties directly to the organization's value"

[Kaplan and Norton, 1996a]. While the financial perspective deals with the projected value of the organization, the innovation and growth perspective sets measures that help the organization compete in a changing business environment. Their focus for this innovation is in the formation of new, or the improvement of existing products and processes.

Through the use of these various perspectives, the BSC provides a more balanced view of the organization's performance [Johnson and Beiman, 2007]. These perspectives are designed to be integrated to achieve the organization's vision and strategy [Beasley et al., 2006]. As Ernst & Young state: "the BSC helps a company to translate its vision and strategy into a clear and balanced set of financial and non-financial KPIs that can be measured" [Ernst & Young, 2009]. These KPIs are cascaded throughout the organization.

From a top-down perspective, one KPI at a higher level is granulated into various, more detailed KPIs at a lower level. For example, at the top of the pyramid sits the "dashboard" BSC for the top management, with a limited number of KPIs. We think the BSC can be seen as a key link between different levels of management and between long- and short-term objectives.

B.4 Performance Prism (PP)

Many alternatives continuous to be developed based on the BSC. The Performance Prism (PP) is an example of one such BSC alternative [Neely et al., 2002]. In the PP, management view their organizations from five perspectives, rather than the four traditional perspectives of the BSC. The PP is depicted in Figure 25. Each area of the prism represents one perspective.

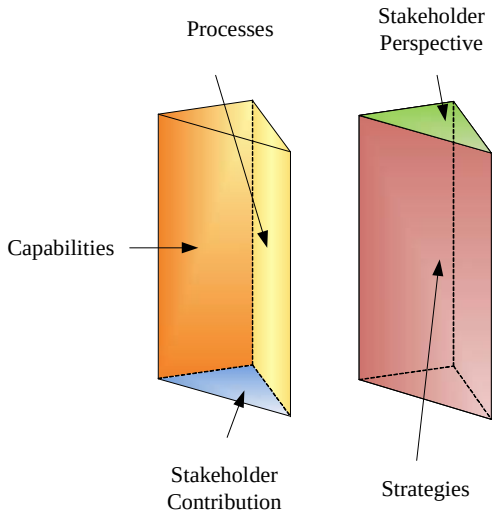

Figure 25: The Performance Prism (PP), from [Neely et al., 2002].

The PP is relatively new, having been developed in 2000 and finding its first significant implementation in 2001. For this reason not many organizations are using the PP yet, they currently stuck most of the time with the BSC.

B.5 Quality Management (QM)

Over the past few decades, many organizations have adopted various quality programs, such as Total Quality Management (TQM), Six Sigma, European Foundation of Quality Management (EFQM), and The Baldridge National Quality Program. Such quality programs aim to assist organizations to improve the quality of the manufacturing and service offerings and thereby improving the performance of the organization [Johnson and Beiman, 2007].

For example, EFQM measures businesses based on even more criteria then the BSC and PP. Nine in total as illustrated in Figure 26. Five of these are enablers (leadership, people, policy strategy, partnership & resources, and processes) and four are results (people results, customer results, impact on society results and business results). The enabler criteria cover what an organization does and the result criteria cover what an organization achieves.

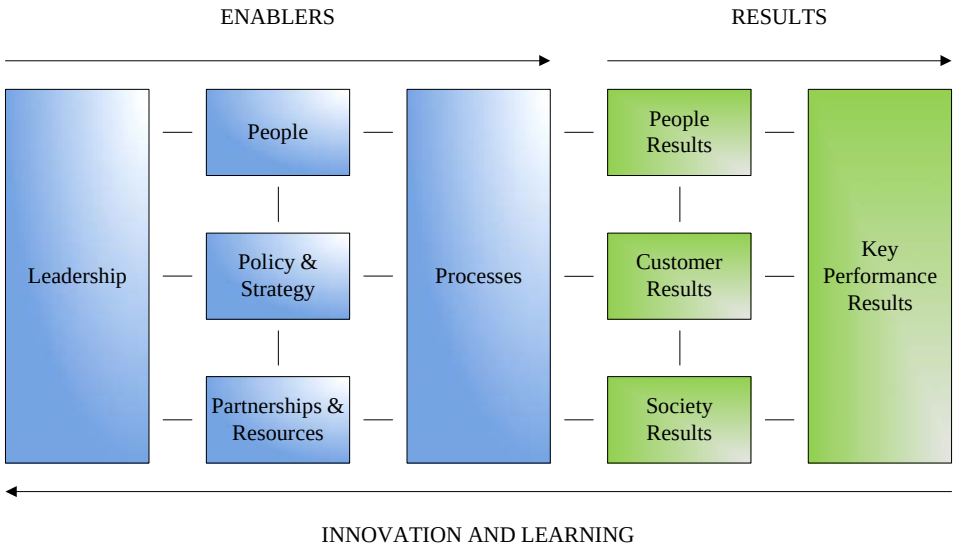

Figure 26: European Foundation Quality Management (EFQM), from [Nabitz and Klazinga, 1999]

The arrows depicted in Figure 26 emphasize the dynamic nature of the model. They show that innovation and learning help to improve enablers which in turn lead to improved results.

C Interview Framework

This section will provide the reader with an interview framework in which the interview questions, methodology, approach and interviewees will be described.

C.1 Interview Objectives

The interviews will be conducted to achieve the following objectives:

- define the current situation about CA & CM, RM and PM;
- define the current relations between CA & CM, RM and PM;
- define the current added value of CA & CM for PM;
- get the interviewees' view about theoretical findings as discussed in Part III;
- enable later contact for validation of findings.

C.2 Interview Methodology

All interviews are scheduled for an hour and a half. Interviewees do only receive some background information about CA & CM, RM and PM and the question about the current situation, but do not receive information about the theoretical findings. There are some reasons not to do so:

- we provide theoretical background information to align the terminology between the interviewer and the interviewees;
- we provide the questions to give the interviewee an idea about the questions, so he can think about the answer to speed up the interview;
- we assume that most interviewees do not have time to look at the theoretical findings on beforehand;
- we want to see the first reaction of the interviewees when we present the theoretical findings, to see how complex and credible they are and if it is possible to understand it immediately;
- we want to make sure that interviewees directly understand the model, instead of making their own assumptions and reasoning about it.

We are going to record all interviews (if they are correct with this) and make notes as well. The notes will be the basis for our analysis and the audio material will be used as additional information to dive deeper into a specific topic. All interviewees will receive the analysis and must approve it before we will use it in this thesis. The interviews will take place between the 1 of December and the first of January 2010.

C.3 Interview Approach

The interviews will be conducted following the sequence below:

1. get to know each other;
2. get information about interviewees' role and experience in the organization regarding CA & CM, RM and PM.
3. explain the goal of the research:
    - *show the added value of Continuous Auditing (CA) & Continuous Monitoring (CM) for Performance Management (PM).*
4. current Situation:
    - CA & CM;
    - RM;
    - PM;
    - relations CA & CM, RM, and PM;
    - added value for PM.
5. validation of perceived added value:
    - validate linkages CA & CM, RM, and PM;
    - validate perceived added value for PM.
6. wrap up and explain way forward:
    - summarize;
    - future contact to validate understandings and findings.

C.4 Interview Questions

Experience and Knowledge Interviewee

1. Wat is uw rol in de organisatie?
2. Wat is uw ervaring met CA & CM, RM, and PM?

Current situation CA & CM

1. Wat zijn de drivers achter CA & CM geweest (interne controle, risk, performance)?
2. Welke processen (primaire/secundaire) worden gemonitord met CA & CM?
3. Hoeveel procent van de controls zijn geautomatiseerd in deze processen?

4. Worden deze processen gefaciliteerd door standaard IT systemen (SAP, Oracle, etc)?
5. Heeft de organisatie een gecentraliseerd IT landschap of een gedecentraliseerd IT landschap?
6. Hoe is CA & CM hierin ingericht?
7. Maakt u hierin onderscheid tussen CA & CM?
8. Hoe is CA & CM ingebed in de organisatie structuur (verantwoordelijkheden, meetings)?
9. Hoe worden control indicatoren genoemd?
10. Op welke frequentie worden deze controls gemonitord?

Current situation RM

1. Hoe worden risico's gemanaged?
2. Wordt er gebruik gemaakt van een standaard tool, methode of framework?
3. Is deze aanpak gebaseerd op de doelen van de organisatie?
4. Op welk niveaus gebeurd dit (strategisch, tactisch, of operationeel)?
5. Welke processen (primair/secundair) worden gemonitord?
6. Hoe is RM ingebed in de organisatie structuur (verantwoordelijkheden, meetings)?
7. Op welke type risico's is RM gefocust (strategisch, financieel, operationeel, compliance)?
8. Is de huidige RM aanpak een iteratief proces (worden en reviews uitgevoerd op de huidige aanpak)?
9. Hoe worden risico indicatoren genoemd?
10. Worden deze indicatoren automatisch of handmatig gemonitord?
11. Op welke frequentie worden deze metingen uitgevoerd?

Current situation PM

1. Hoe managed de organisatie de performance?
2. Wordt er gebruik gemaakt van een standaard tool, methode of framework?
3. Is deze aanpak gebaseerd op de doelen van de organisatie?
4. Op welk niveaus gebeurd dit (strategisch, tactisch, of operationeel)?

5. Welke processen (primair/secundair) worden gemonitord?
6. Hoe is PM ingebed in de organisatie structuur (verantwoordelijkheden, meetings)?
7. Is de huidige PM aanpak een iteratief proces (worden en reviews uitgevoerd op de huidige aanpak)?
8. Hoe worden performance indicatoren genoemd?
9. Worden deze indicatoren automatisch of handmatig gemonitord?
10. Zijn deze indicatoren financieel, niet financieel of allebei?
11. Op welke frequentie worden deze metingen uitgevoerd?

Current Added Value CA & CM for PM

1. Vanuit welk oogpunt is er begonnen met het implementeren van CA & CM (control, doelen organisatie, risico's)?
2. Op welke wijze heeft CA & CM invloed op RM?
3. Zijn de KCIs die worden gemonitored met CA & CM gerelateerd aan de KRIs van RM?
4. Welke type risico's worden er gemonitord met CA & CM?
5. In welke processen (primair/secundair) worden deze risico's gemonitord met CA & CM?
6. Zijn de KRIs van RM gerelateerd aan de KPIs van PM?
7. Geven KRIs van RM betrouwbaarheid aan de KPIs van PM?
8. Heeft CA & CM ook direct invloed op PM (Gebruikt de organisatie CA & CM om KPIs te monitoren)?
9. Denkt u dat het model afgebeeld in Figuur 9 van Sectie 9 toepasbaar is in deze organisatie?

C.5 Interviewees

The interviewees of the three Dutch organizations come from a lifting and transport organizations (A), an international life science and performance materials organization (B), and a governmental agency (C). In this research we will express the organizations as "organization A, B, or C".

We furthermore interviewed three experts: one on the CA & CM area, one on the RM area, and one on the PM area. We will call them "... expert", for example, if we talk about CA & CM, we will express the expert as "the CA & CM expert".

We furthermore visited two seminars about CA & CM. The information gathered during these seminars will be used to create information completeness.