CONTINUOUS RISK MONITORING AND ASSESSMENT: CRMA

By

DAEHYUN MOON

A dissertation submitted to the

Graduate School-Newark

Rutgers, The State University of New Jersey

In partial fulfillment of requirements

For the degree of Doctor of Philosophy

Graduate Program in Management

Written under the direction of

Dr. Miklos A. Vasarhelyi

And approved by

_____

Dr. Miklos A. Vasarhelyi (Chair)

_____

Dr. Dan Palmon

_____

Dr. Alexander Kogan

_____

Dr. John Peter Krahel

Newark, New Jersey

January, 2016

ABSTRACT

Continuous Risk Monitoring and Assessment: CRMA

By Daehyun Moon

Dissertation Director:

Dr. Miklos A. Vasarhelyi

In their monograph "Continuous Assurance (CA) for the Now Economy," Vasarhelyi et al. (2010) introduce Continuous Risk Monitoring and Assessment (CRMA) as a future area of continuous auditing. CRMA is a CA methodology to monitor an organization's business risks, identify its uncontrolled significant risks, and prioritize the audit and risk management control procedures for the timely mitigation of such risks. They argue that development of CRMA procedures is necessary to keep maintain the relevance of CA system in a changing audit risk environment.

This dissertation discusses the development of CRMA and proposes a methodology encompassing four components: (1) identification of the risks to be monitored, (2) development of relevant Key Risk Indicators (KRI, Institute of Operation Risk, 2010) for each identified risk, (3) continuous assessment and aggregation of the KRIs developed for each risk in order to measure their exposure levels, and (4) algorithmic prioritization of the audit and risk management procedures to minimize the organization's risk exposure level overall. This framework will assist the auditor in building a risk based CA

system that continuously monitors the exposure levels of the organization's risks, identifies emerging high risks and automatically directs other CA procedures to focus on the areas of high risk exposures in the organization, thereby keeping a CA system relevant and robust to the organization's constantly changing risk environment. Addressing those four components guided the development of the proposed methodology of CRMA.

To illustrate the use of KRIs in monitoring and assessment of an organization's business risk exposure level, we discuss how a corporate reputation risk level can be measured through KRIs under the proposed CRMA methodology. We also present a metric that measures the degree of negative public perception of an organization extracted from current social media platforms (specifically, Twitter) as a KRI to represent the organization's current reputation level and confirm the occurrence of the organization's reputational damage. We demonstrate the present KRI with Twitter response to two real risk events: Purina's lawsuit for selling harmful dog food and Starbucks' "Race Together" campaign. We analyze the Twitter response mentioning these two risk events and measure the degree of the public's negative perception embedded in them by using the present KRI. We discuss our methods used to perform this analysis and present the results.

Acknowledgement

I would like to express my sincere gratitude to my dissertation advisor, Professor Miklos Vasarhelyi for his guidance, encouragement and unwavering support during my doctoral studies. I deeply appreciate for his mentorship, patience and all helpful inputs which enabled me to finish my doctoral studies.

I also would like to express my deepest appreciation to other members of my dissertation committee, Professor Dan Palmon, Professor Alexander Kogan, and Professor JP Krahel for their incredible patience, constructive comments and constant support. Especially, I am very grateful to Professor JP Krahel for his editorial advice and assistance.

Last but not least, I would like to take this opportunity to thank my wife and parents for their unfailing love, patience and support. Without them, I would never been able to complete my dissertation.

Dedication

To my wife, Nahyoung and our children, Daniel and Jonathan

Table of Contents

Chapter 2: Evolution of Risk Based Audit

Chapter 3: CRMA Methodology

Chapter 5: Summary, Contributions, Limitations and Future research

List of Figures

List of Tables

Chapter 1: Introduction, Research objectives and Outline

1.1 Introduction

1.1.1 Business risk audit

Ubiquitous Internet access, globalization, sophisticated financial instruments, and increasingly interrelated economic systems have made an organization's business risk environment more complex and unpredictable. As a result, organizations now face more uncertainties and their business risks are constantly changing. The dynamic nature of modern business risks complicates the processes of auditing business risks and selecting audit procedures. Methods that incorporate an auditor's analysis of an organization's strategy and business risks into audit risk assessments and planning processes are collectively referred to as Business Risk Audit (hereafter, BRA) methodologies (Bell et al., 1997, 2002; Jeppesen, 1998; Robson et al., 2007; Peecher et al., 2007; Curtis and Turley, 2007; Eilisfsen et al., 2001; Knechel, 2007; PCAOB, 2005; Allen et al, 2006; Knechel et al., 2010).

In BRA, risks that threaten the achievement of an organization's strategies and related objectives are considered as the drivers of audit risks (Lemon et al, 2000; Knechel, 2007; Curtis and Turley, 2007). Therefore, the analysis of the client's business models, strategy, and related business risks must to be performed in order to identify the likely sources of audit risks in a BRA practice (Robson et al., 2007). The BRA auditor must understand the client's business strategies and related risks, and evaluate the effectiveness of the 'high-level controls' or 'supervisory controls' that mitigate these risks (Curtis and Turley, 2007). Then, the BRA auditor acknowledges the client's uncontrolled significant business risks ('residual risks'), assess their impact on relevant audit risks, and incorporate them

into audit risk assessment and planning (Bell et al., 1997; Eilisfsen, 2001; Knechel, 2007; Bell et al., 2002; Peecher et al., 2007).

BRA differs from the traditional 'transaction based audit'[1] which conducts audits through an 'accounting lens' (Bell et al., 1997, p.2) and focuses solely on the nature of account balances, classes of transactions, and the client's financial reporting systems in order to assess the risk of material financial misstatements. The BRA methodology takes a 'top-down' audit approach focusing on the client's competitive business environment, strategies, and critical business processes, then moving down to specific financial statement account balances, transactions, and financial reporting controls (Robson et al., 2007). Consequently, the BRA method focuses more on the client's high level controls in association with their risk management processes and corporate governance, which go beyond the financial reporting systems controls (Knechel, 2007; Knechel et al., 2010; Curtis and Turley, 2007).

Current auditing standards employ BRA processes (Knechel, 2007; Robson et al., 2007). For example, Statements on Auditing Standards (SAS) No. 104 through 111 (AICPA, 2006c) require auditors to obtain an in-depth understanding of an audited organization's business industry and related risks that may affect the achievement of the organization's strategies and to assess their potential impacts on audit risks and audit items to be tested. PCAOB also has adopted the BRA process by accepting those new risk assessment standards. For instance, PCAOB Auditing Standards (AS) No. 5 and No. 12 emphasize the top-down approach that requires auditors to evaluate the client's high level internal

[1] Traditional audit approach is also referred to as 'transaction oriented' (Peecher et al., 2007), 'transaction based' (Robson et al., 2007), or 'transaction cycle focused' (O'Donnell and Schultz, 2003).

controls first and move down to significant controls to test and the auditor's understanding of the client's business and its environment as well as related business risks to better identify the material misstatements in their financial statements and relevant disclosures (PCAOB, 2005, 2007). Although AS No. 5 states that the auditor's requirement for the internal control audit is limited to the client's financial reporting process, the researchers argue that examining internal controls over the financial reporting process necessarily lead to analysis of the client's transaction controls, which is essentially same as the business transactions and process controls evaluation, reflecting the BRA approach (PCAOB, 2007; Knechel, 2007).

The traditional, annual audit risk assessment process performed in the audit-planning phase (Robson et al., 2007, p.413) would not effectively recognize changes in an organization's business risks that could occur at any time during the audit, and it is therefore not appropriate for the BRA method. An ongoing risk assessment would be necessary to enable the BRA auditor to recognize changes in the organization's risk profile and promptly reflect them into audit risk assessments and audit planning (Knechel, 2007). Some researchers also note that integrating the client's self-assessment of business risk and high level control into the audit evidence supporting the auditor's decisions and opinions is an imperfect and ambiguous process, further complicating BRA implementation (Knechel, 2007; Robson et al., 2007; Curtis and Turley, 2007).

1.1.2 Need for ongoing risk assessments and linkages business risks to audit risks

Although implementing BRA is challenging, current auditing literature lacks guidance on how a risk based auditor assesses and monitors the client's constantly changing business risks and links such assessments to relevant audit risk impacts and corresponding audit

plans (Knechel, 2007; Robson et al., 2007; PCAOB, 2005). In this dissertation, we address this gap and propose a methodology that enables a risk based auditor to monitor the client's business risks in an ongoing manner, identify emerging risks, and promptly link them to relevant audit risks and audit procedures as well as related risk management procedures for the client's management to take actions to mitigate adverse effects of those emerging risks.

We draw the proposed methodology from the Continuous Risk Monitoring Assessment (hereafter CRMA) concept which was introduced by Vasarhelyi et al. (2010). CRMA was introduced as a new Continuous Assurance (hereafter, CA) procedure that aims to continuously monitor and assess the entity's business risks and prioritize audit and risk management procedures to make CA systems more robust (Vasarhelyi et al., 2010). We argue that such CRMA procedures would help the BRA auditor to monitor and assess the client's business risks in a more real time manner, thereby more timely detecting the client's emerging risks and their impacts on audit risks.

1.1.3 Continuous Risk Monitoring and Assessment: CRMA

Vasarhelyi et al. (2010) initially lay out the concept and motivation of CRMA: monitoring and assessing an entity's risk exposure levels and prioritizing audit *and* risk management procedures focusing on the entity's high risk areas in a more real-time manner. Figure 1 depicts the essence of the CRMA procedures which can be divided into four activities. First, the client's business risks classified as operational, environmental, or black swan (Teleb, 2010). Second, the current statuses of those risks are assessed in real time through continuous monitoring of their relevant Key Risk Indicators (KRIs, IOR, 2010). Third, significant changes are assessed and recognized in an ongoing manner.

Forth, corresponding audit and risk management procedures are prioritized on an ongoing basis to selectively examine the high audit risk areas affected by the client's high risks and related controls, so that the audit risks are reduced and the client's high level risks are mitigated.

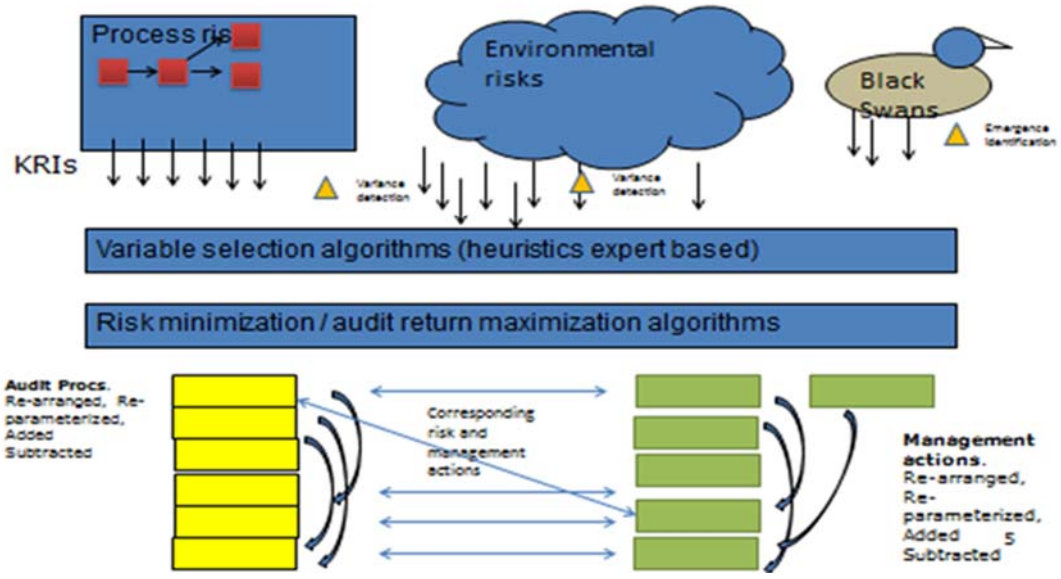

Figure 1 CRMA concept (Excerpted from Bumgarner and Vasarhelyi (2014, p.15))

Vasarhelyi et al. (2010) envisage that CRMA would shift CA to a risk based, dynamic process that promptly deals with the organization's rapidly changing business and audit environment. They call for more research on further developing methods and procedures for CRMA.

We view CRMA as a systematic approach to building a continuous risk assessment and dynamic audit planning process to address business risks and link them to audit and risk management procedures. Such an approach would not only enable a dynamic, risk based

CA system, but also facilitate the BRA process and improve the auditor's ability to detect changes in the client's business risk profile and their impacts on audit risks in a more real time manner.

1.2 Research Objectives

The objective of this dissertation study is to describe the key concepts and background of CRMA and propose a methodology that would provide guidance to implement such key concepts of CRMA. The proposed CRMA methodology provides a set of procedures to implement the suggested conceptual CRMA model (Vasarhelyi et al., 2010) and build a continuous risk assessment and dynamic audit planning process for the BRA practice.

1.2.1 Background of risk based audit

We first provide a literature review on the background of the BRA method, practice, and related auditing standards. As previously mentioned, although BRA has been widely adopted and implemented, there a is lack of guidance on the ongoing risk assessment and linking processes that are critical to effective BRA implementation (Bell et al., 1997; Knechel, 2007; Robson et al., 2007). The proposed CRMA methodology may provide guidance on how an auditor should monitor and assess the client's constantly changing business risks and link them to subsequent audit risk analysis and relevant audit procedure planning decision.

1.2.2 Overview on CA

After reviewing the background of BRA, we review CA procedures and the background of CRMA. We discuss how CRMA would relate to other CA components such as Continuous Data Assurance (CDA) and Continuous Control Monitoring (CCM). Then we present our CRMA methodology which is divided into four procedural steps: (1)

identification of entity risks, (2) selection of relevant key risk indicators (KRIs, Institute of Operational Risk, 2010), (3) use of relevant KRIs to assess the entity's risk exposure levels, and (4) prioritization of audit and risk management procedures in real time. Addressing those four components guided the development of the proposed methodology of CRMA.

1.2.3 Developing CRMA methodology

The proposed CRMA methodology utilizes Key Risk Indicators (KRIs, Institute of Operational Risk, 2010) to monitor the entity's current business risks exposure levels in a real time manner (Hwang, 2010). KRI is any type of data that provides information about the current status of given risk (IOR, 2010). Well-designed KRIs would capture various symptoms and conditions that appear when a risk is developing in a real time manner (Hwang, 2010; Matz, 2008). The continuous monitoring of well-developed relevant KRIs would reveal when the relevant risk is emerging in a real time manner.

We use reputation risk to illustrate the use of relevant KRIs to assess and monitor an entity's risks. From the risk perspective, an organization's damaged reputation may be viewed as a significant business risk event that could affect the achievement of their objectives (Eccles et al., 2007). If an organization's reputation risk exposure level is elevating significantly, a risk based auditor would need to assess which areas are likely to be affected due to the heightened reputation risk and investigate the potential for material misstatements or non-compliance.

1.2.4 Sentiment analysis on Twitter data

Big Data enables the use of KRIs to monitor and assess an organization's significant business risks in real time. To illustrate, we develop a KRI that represents the public's negative perception of an organization measured from real time social media data. For

example, an increasing number of negative sentiments expressed in Twitter messages may indicate a symptom that the reputation of the related organizations may have been damaged.

As such, the present KRI would help to assess and monitor the effect of the organization's reputational risk events. The proposed KRI would contribute to the assessment of an organization's current reputation level and the timely recognition of their reputation damage. We demonstrate the present KRI by measuring it from Twitter messages in relation to two real risk events. First risk event is about the Purina's lawsuit for selling harmful dog food (CNN, 2015). Such event may result in the public's negative perception of Purina, thus affect its reputation. Second risk event concerns Starbuck's "Race together" campaign which involves writing "Race together" on coffee cups and promoting conversations about 'race inequality' or 'race discrimination' with customers. Although the campaign was claimed to help the society to improve race tensions, it faced strong criticisms and received large attentions from mass media. The criticisms were related to the campaign's inappropriateness to ask customers to think or express their opinions on such delicate racial issues at public places and the public's misconception that the campaign was intended for a marketing ploy rather than for a social campaign purpose (WSJ, 2015). Such criticisms could affect the images of Starbucks and hurt its reputation. To demonstrate the present KRI representing the effect of a risk event on the public's negative perception, we measure it from the Twitter data mentioning these particular risk events.

1.3 Research Contributions

The contributions of this dissertation study are twofold. First, the present study contributes to CA research. Vasarhelyi et al. (2010) point out that since an organization's business and audit environment change constantly, and that contemporary audit standards require a risk based approach, today's CA system should be risk driven and dynamic. They suggest developing a CRMA system that continuously monitors and assesses an organization's risks and prioritizes audit and risk management procedures. We refine the essential concepts of CRMA and propose a methodology to operationalize such CRMA concepts for the first time.

Second, a lack of guidance on continuous risk assessment is a major obstacle to implementing an effective BRA process. We develop a CRMA methodology that involves ongoing risk assessment and linking the client's business risks to relevant audit and risk management procedures. The proposed CRMA methodology suggests a new approach to building a continuous risk assessment process and develops a linking mechanism between the client's business risks assessments and the relevant audit risk assessments for an effective BRA process. As such, the present study on CRMA contributes to the BRA literature.

The remainder of the paper is organized as follows: Chapter 2 discusses the current trend in audit risk assessment standards that emphasizes incorporating the client's business risk assessments into the subsequent audit planning process and into the widely practiced BRA method. Such a trend suggests an evolution of audit risk assessment, which has transformed from a periodic and accounting-error-focused risk assessment practice to an ongoing and business-risk-focused risk assessment process. Chapter 3 proposes a CRMA

methodology that consists of four procedural steps to assess an organization's various risks and update the audit procedures as an organization's risks change in a real-time manner. Chapter 4 discusses monitoring and assessing an organization's reputation risk using relevant KRIs under the proposed CRMA methodology. Chapter 4 also presents a KRI that measures the degree of public's negative perceptions of an organization extracted from real time based social media platforms such as Twitter, which would help to understand the organization's current reputation level and detect any significant reputational damage occurred in a more real time manner. We measure the present KRI on Twitter messages for two real risk events. Chapter 5 concludes the study with a discussion of the implications, limitations, and future research agenda of the development of CRMA.

Chapter 2: Evolution of Risk Based Audit

2.1 Business Risk Audit (BRA)

2.1.1 Background

Due to deregulations on competitive bidding and increased competition during the 1980s and 1990s (Kinney, 2005, p.91; Zeff, 2003a, p.202), major audit firms have strived to streamline their services and improve audit quality (Knechel, 2007; Robson et al., 2007). Also, a growing interest in Enterprise Risk Management (ERM) has led many organizations to replace individual- or department-based risk management practices with enterprise-wide, integrated risk management processes (Knechel, 2007). Under such intensified competition, public audit companies have reengineered their existing audit methods to integrate the client's risk management related functions (e.g. identification, measurement, and monitoring), into the formal audit process (Lemon et al., 2000; Bagshaw, 1999; Knechel, 2007; Robson et al., 2007) [2]. Such new audit methods developed in the 1990s are collectively referred to as 'Business Risk Audit (BRA)', 'Strategic Systems Audit', or 'Risk Based Audit' (Bell et al., 1997; Peecher et al., 2007; Knechel, 2007; Robson et al., 2007).

Under the BRA[3] approach, the audit risk assessment process is viewed as an evidence-driven, belief-based risk assessment process (Peecher et al., 2007). The BRA auditor first analyzes the client's business strategies, environment, process and related business risks to develop his or her beliefs with the audit risk assessments. Bell et al. (2005) describe

---

[2] BRA audit techniques developed by major audit companies include Business Audit (Arthur Andersen), Audit Innovation (Ernst & Young), Business Measurement Process or BMP (KPMG) and PwC Audit Approach (PricewaterhouseCoopers)(Robson et al., 2007; Knechel, 2007; Lemon et al., 2000)

[3] We collectively refer those business risk based audit methodologies as BRA (Business Risk Audit).

this approach to obtaining audit evidence as 'evidentiary triangulation' which involves iteratively developing and revising expectations about a client's financial statement representations by understanding fundamental sources of the 'entity business states (EBS)'[4]. They argue that addressing whether such 'EBS' are fairly conveyed through management information systems and reflected in business performance and financial statement representations is the best way to detect management fraud and hidden material misstatements (Bell et al., 2005; Peecher et al., 2007).

Such a BRA approach involves 'systems-thinking' perspective or a 'strategic-systems' lens (Bell et al., 1997) through which the auditor understands and finds the fundamental sources of the audit risk. 'Systems-thinking'[5] in the BRA context is to understand the organization's internal and external environments, business strategies, and processes to create value, interrelationship with internal and external constituents. It requires the auditor to understand the organization's business risks to threaten to fail the strategic objectives and goals of the organization in order to develop their beliefs about the audit risks (Bell et al., 1997; Bell et al., 2005; Peecher et al., 2007).

Proponents of the BRA approach argue that such 'systems-thinking' would enable auditors to obtain more powerful sources of evidences to evaluate the fairness of an organization's financial statements (Bell et al., 1997; Peecher et al., 2007; Knechel, 2007).

---

[4] "Entity business states (EBS) are the business strategies, conditions, processes, and economic actions/events and relationships with other entities that pertain to the audited entity and its economic web" (Bell et al, 2005, p.4)

[5] Systems thinking is characterized as "the language, cognitive tool set, and perspectives that enable decision makers to form reasonably accurate and complete mental representations of complex environments" (Hecht, 2004, quoted in Peecher et al., 2007, p.471). Systems thinking is employed in Strategic Systems Auditing (SSA) which is considered as the first academic contribution introducing the BRA method in the literature (Kinney, 1997).

BRA is considered an innovative audit approach as it shifts from a focus on accounting transactions and relevant audit risks into business risk- based audit that involves understanding the veracity of the client's business strategies and objectives, business processes, and relevant business risks to decide audit risks and further audit plans to be performed (Kinney, 1997; Peecher et al., 2007; Robson et al., 2007).

2.1.2 Top-down approach and Value added audit

The BRA method takes a holistic and top down approach to understanding the audit risk involved in the auditee's organization (Knechel, 2007; Curtis and Turley, 2007; O'Donnell and Schultz, 2005) (Table 1). As aforementioned, the BRA method requires the auditor to first understand the client's business strategies and objectives, and the related risks that could affect the client's ability to achieve them. Then the auditor examines the effectiveness of the relevant internal controls to evaluate whether they are effectively designed and implemented to mitigate the adverse consequences of the client's business risks and identifies 'significant risks' or 'residual risks' (Bell et al., 1997; Bell et al., 2005; Knechel, 2007) whose controls are either ineffective or absent. The auditor then plans subsequent audit procedures addressing potential audit problems stemming from such significant risks (Bell et al. 1997; Ballou et al. 2004; Knechel, 2007). As such, BRA dictates the auditor to work from the top, examining the viability of the auditee's strategies and objectives and related risks holistically first and then narrowing down to areas of high audit risk and designing further audit procedures for those areas. (Knechel, 2007; Robson et al., 2007; Peecher et al., 2007).

The proponents of the BRA method argue that the top-down approach improves audit effectiveness and efficiency, creating more value for the client. BRA may increase audit

risk assessment effectiveness at finding hidden audit related risk factors, such as management's motivations to perpetrate fraudulent financial reporting, going concern issues, and ineffective internal controls (Bell et al., 1997; Bell et al., 2005; Peecher et al., 2007). The BRA approach promotes the auditor to consider the root causes of audit concerns, which are often originated from the organization's unmanaged business risks; it therefore provides a better evidential basis to determine the risk of material misstatements and increases audit effectiveness (Bell et al., 1997; Peecher et al., 2007).

The BRA approach would also reduce substantive audit procedures to be undertaken, so that it facilitates a more efficient audit process (Eilifsen et al., 2001; Bell et al., 1997; Bell et al., 2005). BRA requires auditors to evaluate the effectiveness of the organization's high level controls in association with their business processes and risk managements, and then assess audit risks and plan subsequent audit procedures. This top-down approach is expected to obviate the need for needless substantive procedures, allowing the auditor to focus on only high risk items and reducing the scope of substantive audit procedures to be performed (Eilifsen et al., 2001; Ballou and Knechel, 2002; Curtis and Turley, 2007). However, results from empirical studies on this topic are mixed. For example, Eilifsen et al., 2001 document from their case study that traditional substantive testing was decreased since a BRA method adopted. On the contrary, Curtis and Turley (2007) found that the same substantive audit procedures were applied even after a BRA approach was adopted, suggesting that implementation of the BRA method is difficult.

Third, the proponents of the BRA method claim that it provides 'value added' audit service (Bell et al., 1997; Peecher et al., 2007). They argue that as the BRA method requires the auditor to understand the client's business strategies, processes and related

risks, such understanding about the client's business processes and risk management effectiveness can be provided as a valuable feedback (Bell et al., 1997; Bell et al., 2005). The auditor's knowledge "spillover" (Robson et al., 2007) and insight into the client's business risks and related control effectiveness would be valuable for the client to evaluate its risk management effectiveness in an objective manner. The BRA approach results in a 'value added' audit, while the traditional audit is 'compliance-oriented' (Eilifsen et al. 2001; Lemon et al. 2000; Robson et al., 2007).

The top-down approach to conducting an audit has been adopted in current auditing standards such as Statements on Auditing Standards (SAS) No. 109 and the PCAOB's Auditing Standards (AS) No. 5 (Knechel, 2007, PCAOB, 2007). We discuss these standards later in this chapter.

Top-down Approach of Business Risk Audit

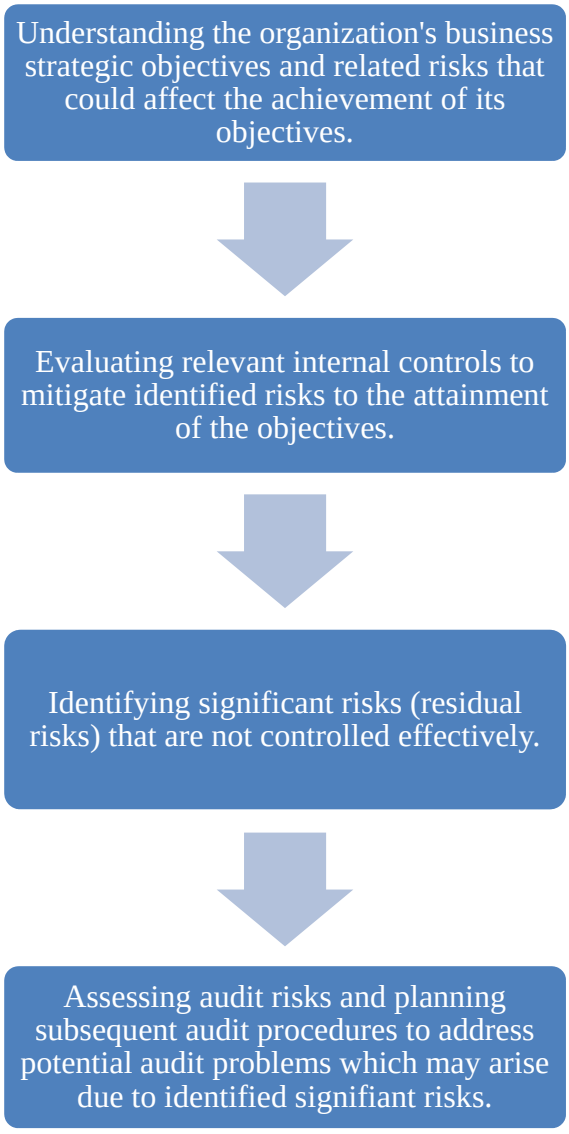

Table 1 Top-down approach of business risk audit method (Curtis and Turley, 2007; Knechel, 2007; Robson et al., 2007)

2.1.3 Business risks drive audit risks

The assumption that "business risk drives audit risk" is central to the BRA method (Lemmon et al., 2000; Eilifsen et al.,2001). This implies that the organization's unmet business objectives, inefficient processes, or related unmanaged risks are also audit risk factors that may lead to problems such as inappropriate accounting practices, fraudulent financial reporting, or ineffective internal controls.

For example[6], increasing production costs due to the rising of oil price would be a business risk for a plastic products maker, increasing the company's production costs and reducing profit margins. In this case, the company could anticipate and manage such a risk by entering future contracts or increasing prices and passing the risk on to the customer. If such risk management related internal control exists and functions effectively as intended, the company may ensure profitability even if the underlying risk event (oil price increases) occurs. On the contrary, if the company fails to anticipate such a risk and does not prepare relevant risk control activities, the abruptly increased oil price may lead to a failure to achieve its targeted performance level or induce significant operating losses. Consequently, the manager who did not achieve the expected target performance may engage in inappropriate accounting practices such as 'channel stuffing' to conceal underperformance (Knechel, 2007, p.395).

As such, an organization's unmanaged risks that threaten the organization's strategies and objectives may drive related audit risks. Under the BRA approach, the organization's uncontrolled business risks are viewed as fundamental causes of audit risks. Such business risks whose control activities are not regarded as effective and functioning are often referred to as 'residual risk' or 'significant risk' in the literature (Bell et al., 1997; Bell et al., 2005; Knechel, 2007).

2.1.4 Implications of 'significant risks' ('residual risks') on audit risk

If significant business risks drive audit risks, the BRA auditor must understand the audit implications of the client's significant business risks. That is, the auditor should be able to identify potential audit risks from the client's significant risks profile. Eilifsen et al.

[6] This example is adopted from Knechel (2007)

(2001) discuss the following implications of the organization's significant risks on audit risks:

1) "In the most extreme situation, residual risks could hint at a going-concern problem"

2) "Some residual risks may suggest potential weaknesses in the overall control environment and create incentives for management to undertake inappropriate actions or manipulate information in the financial statements"

3) "Some risks may indicate potential problems in the organization's business processes"

4) "Residual risks may link directly to specific financial assertions indicating heightened inherent risk"

Peecher et al. (2007) also stress that an organization's significant risks may increase the risk of fraudulent financial reporting, thus elevating audit risk. They explain that an organization's uncontrolled business risks make it less appealing to creditors and investors; thus motivations to distort financial performance or relevant disclosures to hide significant threats and manipulate perceived future profitability increase when a firm faces significant uncontrolled business risks. They therefore argue that the risk of material misstatement is dynamic and changes over time as underlying significant business risks change. (Peecher et al., 2007).

"When such threats or business risks increase or spike, management generally faces greater temptation to optimistically distort their business-state representations. Thus, shifts in business risks have audit risk implications. … In auditing parlance, RMM is dynamic as a result of shifting business risks over time. In systems-thinking parlance, the stock of RMM changes over time and the auditor must combat changes in RMM by lowering DR (detection risk) when warranted " (Peecher et al., 2007, p.474).

An organization's significant business risks may also indicate that the organization's internal control system is not effective. According to Committee of the Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated

Framework (2013)[7], control activities are one of the five components that determine the effectiveness of the organization's internal control system. COSO (2013) prescribes that an organization's control activities should be designed to mitigate risks to the achievement of the organization's business objectives. KPMG (2013) reports that the relevant principle adopted in this 2013 internal control framework is as follows:

"the organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels" (KPMG, 2013, p.5).

This may imply that under the COSO framework, the presence of significant uncontrolled risks may be recognized as a signal that the organization's internal control activities are not effective.

COSO's internal control framework has been recognized as suitable for evaluating an audit client's internal control systems (SAS No. 109, AICPA, 2006b; AS5, PCAOB, 2007; Knechel, 2007). Identification of significant risks may indicate a weakness in the client's internal control systems. Although current audit standards related to the internal control audit (PCAOB, 2007) maintain the scope of the audit as the client's financial reporting process, the top-down approach and the business risk-level control activities evaluation would invariably extend such a limited focus on the client's financial reporting process into the client's high level business strategy, processes, risks, and controls.

To provide an example of how a significant business risk may impact audit risk, recall the oil price risk example (Knechel, 2007). In this example, the relevant internal control

[7] COSO updated its 1992 Internal Control Framework (COSO, 1992) and released a new updated internal control framework in 2013 (COSO, 2013). COSO maintains the five components of internal control used in its 1992 framework in its 2013 framework as well, but added the 17 principles to be present and functioning to support the five components (KPMG, 2013).

activities may include switching to different oil suppliers who assure a fixed price, buying insurance, or limiting or adjusting oil purchase schedules, etc. If such controls are effectively implemented to mitigate the adverse effects when the oil price increases abruptly, the organization's oil price risk may not be identified as a significant risk. However, if these internal control activities are not effectively designed and implemented, then the auditor may identify the organization's oil price risk as a significant risk and plan subsequent audit procedures that reflect its implications on audit risks such as going concern, weak internal controls, opportunity for management to distort relevant financial reports, or inherent risks for related financial statement accounts, such as sales (Figure 2).

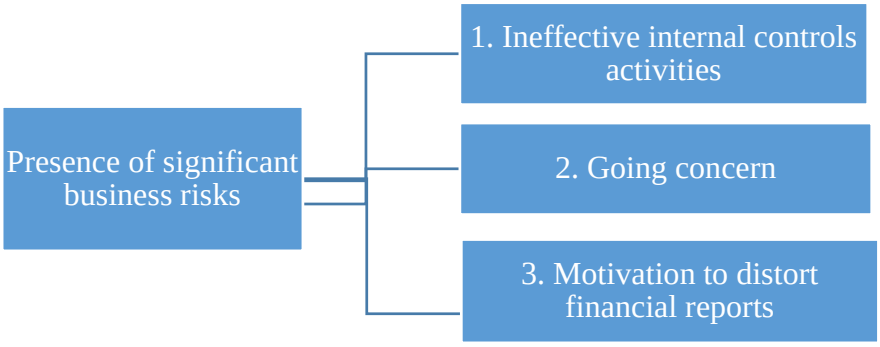

Figure 2 Implications of an organization's uncontrolled significant business risks on audit concerns (Eilifsen et al., 2001)

2.1.5 Methods and Practice

2.1.5.1 Transactions-focused approach (TFA) and Business Risk Audit (BRA) approach

Audit firms use two approaches to conduct audit risk analysis in a risk based audit practice: (1) traditional transactions-focused approach (TFA) which focuses on the client's transactions cycles and the internal controls relevant to the organization's

financial reporting process, and (2) the present BRA approach which involves an analysis of the client's business strategies, objectives, and related risks, as well as the effectiveness of relevant internal controls to identify the risks of material misstatements at account balance and relevant assertion levels (Bell et al., 1997; Robson et al., 2007; Knechel, 2007; Schultz et al., 2010).

Under the TFA approach, the auditor assesses the risks of material misstatements in each transaction cycle (e.g. revenue, expenditure, production, payroll, financing, or reporting) and financial statement account balance (Louwers et al., 2008, p. 95). This approach leads the auditor to focus on transactional events and the relevant financial reporting process without necessarily understanding the business objectives and processes which drive the transactions (Bell et al., 1997). Thus, under the TFA approach, the auditor does not necessarily need to link an understanding of the organization's business related risks and relevant internal controls effectiveness to determine the risks of material misstatements and further audit procedures to be performed.

Unlike TFA, BRA is a top-down approach to assessing the risks of material misstatements and selecting what to be tested. This involves linking the client's business risk assessment to the audit risk assessment (Robson et al., 2007; Knechel, 2007).

Proponents of BRA argue that it makes the auditor much more knowledgeable about the client's business and environment, and therefore better able to identify hidden material misstatements and other audit risk factors. Researchers (O'Donnell and Schultz, 2003; Schultz et al., 2010) find that auditors using BRA better identify seeded risk factors for material financial misstatements than those using the TFA approach. These findings support the importance of understanding of the organization's significant business risks

to the achievement of their strategies and objectives in assessing the risk of material misstatements.

While the BRA method may better detect hidden risks of material misstatements, an organization's business risks are vague and subtle, hindering the auditor's use of results from their business risk assessments as audit evidence to support their audit risk analysis and subsequent audit plans (Curtis and Turley, 2007; Robson et al., 2007; Knechel, 2007).

2.1.5.2 New Audit Skills, Structure, Resources for Business Risk Audit

The adoption of BRA has resulted in changes in audit technology (Robson et al., 2007). To use BRA successfully, the auditor used to TFA should be equipped with new analytical skills and tools (Eilifsen et al., 2001; Robson et al., 2007; Knechel et al., 2010; Bell et al., 2008). Arthur Anderson's Business Audit, Ernst & Young's Audit Innovation, KPMG's Business Measurement Process and PricewaterhouseCoopers' PwC Audit Approach are typical BRA audit methodologies developed in the late 1990s (Robson et al., 2007; Knechel, 2007; Lemon et al., 2000). New techniques and tools needed for BRA include understanding the company's strategies and business processes, evaluating whether relevant risk management-related internal controls are effectively designed and implemented, assessing the potential impacts of the company's significant risks on the areas of the audit, and deciding the appropriate audit procedures that address the potential audit problems that may arise from them.

Furthermore, the BRA auditor would need tools and techniques to promptly recognize changes in the organization's risk profile and their effects on audit risk so that current audit procedures can be timely adjusted to address the potential audit consequences (Knechel, 2007). Researchers envisage that audit structure, resources, and procedures are

expected to change with the adoption of BRA (Eilifsen et al., 2001; Bell et al., 2008; Curtis and Turley, 2007; Bierstaker and Wright, 2004; O'Donnell and Schultz, 2003).

2.2 Audit Risk Model

Current auditing standards have also addressed the BRA method. Risk is a not a novel auditing concept (Knechel, 2007): In the 1970s, the Auditing Standard Boards (ASB) introduced the Audit Risk Model (ARM) which has since guided risk based audit practices (Knechel, 2007; Allen et al., 2006). We first discuss this ARM in general before providing the current BRA-related standards.

The ARM is described as the following equation[8] (SAS No.107, AICPA, 2006a):

*Audit Risk (AR) = Inherent Risk (IR) * Control Risk (CR) * Detection Risk (DR).*

SAS No. 107, AU Section 312 provides a guideline on the use of ARM (AICPA, 2006a). AU Section 312, Para. 2 defines audit risk (AR) as "the risk that the auditor may unknowingly fail to appropriately modify his or her opinion on financial statements that are materially misstated[9]". Para. 12 characterizes AR as "a function of the risk that the financial statements prepared by management are materially misstated and the risk that the auditor will not detect such material misstatement". Para. 21 defines inherent risk (IR) as "the susceptibility of an assertion to material misstatement, assuming that there are no related controls" and control risk (CR) as "the risk that a material misstatement that could occur in a relevant assertion and that could be material, either individually or when aggregated with other misstatements, will not be prevented or detected on a timely basis

[8] SAS No. 107 states that the ARM should be considered as a conceptual tool, rather than a mathematical equation (Para. 26)

[9] This definition of audit risk does not include the risk that the auditor might erroneously conclude that the financial statements are materially misstated. (AU 312, Para 2)

by the entity's internal control". The combination of IR and CR is described as the risk of material misstatement (RMM).

SAS No. 107 and related PCAOB's Auditing Standards (AS) No. 8 require the auditor to perform risk assessments[10] to evaluate the risk of material misstatements[11] and determine further audit plans to achieve a reasonably low level of audit risk (AICPA, 2006a; PCAOB, 2010a).

AU 312 divides the auditor's risk assessment process into three phases: (1) 'risk identification', (2) 'risk analysis (assessment)', and (3) 'auditor response'. In the risk identification phase, the auditor identifies risks that could affect the financial statements and related disclosures. During risk analysis, the auditor assesses IR and CR. In the auditor response phase, the auditor determines overall audit plans (assignment of personnel, level of supervision, etc.) and relevant substantive audit procedures to be performed based on the results of the assessments of RMM.

Under ARM, the auditor first assesses the level of RMM and then determines an appropriate level of Detection Risk (DR)[12] to be. Unlike IR and CR which originate from the client's unique characteristics and business environment, DR arises from improper audit plans or procedures and can be managed by the auditor (SAS No. 107, AICPA, 2006a). SAS No. 107 explains that DR exists due to the limitation from testing samples

[10] PCAOB (2005) describes the auditor's risk assessment as "a process whereby the auditor evaluates the risk that material misstatement will occur and then plans and performs his or her audit based on those evaluations" (PCAOB, 2005, p. 5).

[11] Errors include unintentional misstatements or omissions of amounts or disclosures in financial statements (AU 312, Para 6), whereas fraud arises from intentional fraudulent acts, such as misstatements from fraudulent financial reporting or from misappropriation of assets. (AU 312, Para 7)

[12] DR is often decomposed in AP (DR associated with analytical procedures) and TD (DR associated with tests of details, i.e., substantive testing).

only, rather than 100% of account balance or transactions (sampling risk), misapplication of audit procedures (non-sampling risk), and misinterpretation of audit results (non-sampling risk).

The auditor may adjust the level of DR based on the perceived RMM in order to reduce overall audit risk to an acceptable level. For example, if the auditor believes that the RMM is high, he or she will lower DR by applying more effective and substantive audit tests. Likewise, if the auditor believes the RMM is low, a higher DR and fewer substantive tests may be acceptable. Using the ARM, the auditor finds an optimal level of audit effort to achieve reasonably low audit risk (Waller, 1993; SAS No. 107, AICPA, 2006a).

The ARM has been a prominent tool for risk based audit planning (Libby et al., 1985; Waller, 1993; Allen et al., 2006; Peecher et al., 2007). However, researchers find that auditors often do not assess IR or CR meaningfully, nor do they use the ARM to determine the extent of further audit procedures (Waller, 1993; McConnell and Schweiger, 2007; Allen et al., 2006). For example, Waller (1993) documents that most auditors elect not to rely on the client's controls for efficiency reasons, thereby setting CR at maximum as a default. Although this practice is consistent with professional standards, the effectiveness of such a risk assessment in guiding further audit procedures is questionable. Waller (1993) commented:

"The finding of an insignificant association between IR and CR runs counter to the idea that a knowledge-based dependence exists between the audit risk model's components. This result largely stems from the predominance of cases in which CR is assessed at the maximum. An explanation is that auditors use CR assessments primarily as a way to document decisions about (non) reliance on controls. Though consistent with professional standards, this practice creates doubt about whether the purpose of risk assessment is to guide or confirm the choice of audit procedures" (p.801).

Allen et al. (2006) argue that inherent risks (IR) are not assessed meaningfully. They find that inherent risks are often measured identically for all assertions related to an account and often assessed with CR taken together, implying indifference to IR. Allen et al. (2006) state:

"Also, research on the audit risk model indicates that inherent risk and control risk often get blurred or combined (e.g., Haskins and Dirsmith, 19965; Messier and Austen, 2000). Based on these studies, inherent risk assessments (1) often are not meaningfully applied to each assertions; (2) may be decreasing over time, possibly to promote audit efficiency; and (3) sometimes are combined with control risk into one combined risk factor" (p. 165).

The ARM is also criticized for not addressing the auditor's non-sampling risks[13], considered more relevant to audit failures (Peecher et al., 2007). Peecher et al. (2007) state that;

"Perhaps, in part, because the ARM does not emphasize non-sampling risk, neither audit approaches nor historic audit standards traditionally focus the auditor's attention on the identification and mitigation of non-sampling risk factors (e.g., factors that elevate the likelihood of auditor risk assessment error) … In other words, even though audit risk assessment is quite complex and inevitably subject to assessment error, even by audit experts, the traditional auditor's attention may well be mis-directed away from non-sampling risk, likely to a degree that is detrimental to audit quality" (Peecher et al., 2007, p.468).

To improve the auditor's use of the ARM and risk assessments, the audit standard setters issued new risk assessment standards that adopt the BRA approach (McConnell and Schweiger, 2007; AICPA, 2006c; PCAOB, 2010a). We discuss these standards in more detail in the following section.

[13] Non-sampling risk is "the risk that the auditor reaches an erroneous conclusion for any reason not related to sampling risk". Sampling risk is defined as "the risk that the auditor's conclusion based on a sample may be different from the conclusion if the entire population were subjected to the same audit procedure" (IAASB, 2014, p.26).

2.3 New risk assessment standards emphasizing understanding business environments and related business risks

2.3.1 External Financial Audit

In March 2006, the Auditing Standard Boards (ASB) issued a set of new risk assessment standards: Statements on Auditing Standards (SAS) 104 through 111 (AICPA, 2006c). These new standards are meant to enhance the auditor's application of the ARM by requiring them to obtain a more in-depth understanding of the client organization's business in order to better identify risk of material misstatements (McConnell and Schweiger, 2007). These standards were expected to reinforce the application of ARM as they more explicitly require the auditor to assess IR and CR before planning the audit (McConnell and Schweiger, 2007; Ramos, 2009).

SAS No. 109 explicitly requires the auditor to understand the client's business and its environment (AICPA, 2006b):

> *The auditor must obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures (Para. 29).*

SAS 109 also explains the implications of the entity's business risks on RMM:

> *A business risk may have an immediate consequence for the risk of misstatement for classes of transactions, account balances, or disclosures at the relevant assertion level or for the financial statements taken as a whole. For example, the business risk arising from a contracting customer base due to industry consolidation may increase the risk of misstatement associated with the valuation of accounts receivable. … Furthermore, a business objective and related risks may also have a longer-term consequence that the auditor may need to consider when assessing the appropriateness of the going concern assumption. For example, the business risk of a decline in the industry in which the entity operates may affect the entity's ability to continue as a going concern. The auditor's consideration of whether a business risk may result in material misstatement is, therefore, made in light of the entity's circumstances (AICPA, 2006b, Para. 31).*

SAS 109 also explains the possible effect of the organization's business risk on the financial statement audit[14]:

"[A]n understanding of the company's business risks would increase the likelihood of identifying risks of material misstatements (para. 30)"… Most business risks will eventually have financial consequences and therefore an effect on the financial statements"(AICPA, 2006b, Para. 31).

The Public Company Accounting Oversight Board (PCAOB) has also asserted that the organization's significant business risks may increase RMM (PCAOB, 2010a). For example, Auditing Standards (AS) No. 12 emphasizes that to assess RMM, the auditor must understand the company's objectives, strategies, and related business risks that might reasonably be expected to result in risks of material misstatement (PCAOB, 2010a).

However, the PCAOB (PCAOB, 2010b) remarks that although not all business related risks may result in material misstatements in financial statements, some significant business risks lack controls, posing a greater threat to the achievement of the organization's objectives and goals and increasing RMM. (PCAOB, 2010b).

2.3.2 Internal Control Audit

The PCAOB's Auditing Standard No. 5 (AS5) for the internal control audit also adopt the BRA for controls testing (PCAOB, 2010a). AS5 requires the auditor to use a top-down approach and evaluate entity-level controls. According to AS5, entity-level controls include (PCAOB, 2007, Para. 24):

(1) Controls related to the control environment
(2) Controls over management override

[14] SAS 109 Appendix C lists for the conditions and events that the entity's business risks might come from and that also indicate the risks of material misstatements.

(3) The company's risk assessment process
(4) Centralized processing and controls
(5) Controls to monitor results of operations
(6) Controls to monitor other controls
(7) Controls over the period-end financial reporting process
(8) Policies that address significant business control and risk management practices

The PCAOB (2007) believes that understanding entity-level controls may lead the auditor to reduce the testing of other controls. For example, if the auditor determines that the management's philosophy and operating style (an entity-level control) provide a strong internal control environment, financial reporting process control testing may be less necessary (PCAOB, 2007).

2.4 Audit Risk Assessments for Internal Auditing

Recent accounting scandals and resulting regulation reforms have expanded the scope of internal audit functions at organizations (Hass et al., 2006; Burnaby and Hass, 2011). For example, Sarbanes-Oxley Act's Section 404 requires publicly traded companies to design and maintain effective internal control systems, signifying a need for the internal audit functions to assist in compliance (Rezaee, 2010). The New York Stock Exchange (2004) likewise requires trading companies to have an internal audit function (Carcello et al., 2005; Rezaee, 2010).

Risk assessment is critical to internal audit planning (Ramamoorti et al., 1999). The IIA's (Institute of Internal Auditors) Performance Standards (2010) explicitly state that the internal auditor must develop a risk-based plan for all internal audit activities based on the organization's risks assessments and must evaluate the effectiveness of management's risk management process (IIA, 2012). Similar to the audit risk assessment process in the

external audits standards, the process of risk assessment for internal auditing involves identifying auditable activities and relevant audit risk factors and determining subsequent audit plans (Ramamoorti et al., 1999).

For internal audit, audit risk exists for each of three types of internal audit activities that the internal auditor may perform: compliance, operational, and financial. Audit risk in each category is the risk that the internal auditor provides an incorrect opinion for the relevant audit area (Colbert and Alderman, 1995). Similarly, audit risk is also defined as "the risk that the auditor will fail to provide effective, timely, and efficient assurance and consulting support to company management and its board of directors" (Schneider et al., 2012).

Similar to the BRA approach, the IIA Practice Advisory 2010-2 (IIA, 2010) requires the auditor to assess the organization's risk management process and focus on both inherent risk levels (risk levels without considering relevant controls) and residual risk level (risk levels considering related controls), and determine priorities for allocating internal audit resources. Such risk based internal audit planning is similar to the BRA approach.

IIA Practice Advisory 2200-2 (IIA, 2010) mandates the internal auditor to use the top-down approach in identifying 'key controls' that are relied upon to mitigate significant risks. This approach ensures that the internal audit activities are focused on "providing assurance on the management of significant risks" (IIA, 2010).

Unlike the external auditor whose responsibility is mainly to issue an opinion on the fairness of the client's financial statements or effectiveness of internal control systems, the internal auditor works with management and the audit committee to protect and

increase stakeholder value. Internal auditors can act as facilitators to promote the management's CRSA[15] initiatives. Allegrini and D'onza (2003) find that internal audit functions conceive CRSA initiatives as an opportunity to extend their audit coverage to more actively support risk management and controls and increase audit value:

"All the companies that have implemented a CRSA project declare that it helps management, at all levels, to assume responsibility and accountability for effective control and risk management. Some practitioners emphasize that CRSA is a powerful way to improve the organization's control environment. Then, it is generally recognized that CRSA offers lots of benefits for audit departments, because it extends the audit coverage, it helps internal audit to focus on risks and to understand the business" … "Internal auditors attempt to add value through a more active support to risk management at different levels, and to align internal audit objectives with the strategic goals of the organization. This group includes the 'early pioneers' of CRSA projects" (p.199).

2.4.1 Expanded roles of internal audit function: increasing emphasis on assuring the organization's ERM process

Internal auditors have gone from "bean counters" and "number crunchers" helping accounting management in the 1900s, to providing assurance about the internal controls over the accounting process in 1940s, to evaluating operational processes in the 1980s (Bou-Raad, 2000).

However, today's internal audit function is increasingly asked by the management and board executives for more active participation in providing assurance on the effectiveness of the organization's risk management process and contributing to strong corporate governance (IIA, 2009; Schneider et al., 2012; E&Y, 2013).

As discussed earlier, many organizations have adopted ERM to improve their risk management practices. Such initiatives in building an effective risk management process

[15] Control and risk self-assessment (CRSA) describes systematic and participative techniques used by management to identify, classify, assess, measure and evaluate risks and controls (IIA 2004; Jordan 1995; Allegrini and D'onza 2003).

and enhancing corporate governance were viewed as an opportunity to broaden traditional controls-driven internal audit activities to business risks and risk management focused audit functions and promoted the use of risk-based audit approach. Such risk-based audit and risk management-focused audit activities are seen as a mechanism to align internal audit activities with strategic and operational objectives, creating more value-added audit services (Selim and McNamee, 1999; Spira and Page, 2003).

2.4.2 Internal auditor's role in ERM

A recent PwC survey reveals that providing assurance on the management's risk management process and internal control framework would enhance internal audit's value to the organization (PwC, 2015). Internal audit functions are increasingly expected to eliminate routine, low-value audits and contribute to strengthening corporate governance and risk management as strategic partners, expanding their traditional roles (Jackson et al., 2008; PwC, 2015).

Managing business risks is a responsibility of management (Moeller, 2009); management is responsible for building and maintaining an effective ERM process that ensures successful operations. Internal audit should not be accountable for risk management decisions for the organization (Hass et al., 2006). However, Zwann et al (2011) find that internal auditors involved in ERM assurance activities also engage in activities that could compromise the internal auditor's objectivity (Zwann et al, 2011). IIA (2009) explains that any engagement that goes beyond assurance service should be treated as consulting engagements and performed on certain conditions to preserve the independence and objectivity of assurance services. Table 2 summarizes what are acceptable and unacceptable conditions for the internal auditor's assurance activities

Acceptable	• Reviewing management of key risks • Evaluating key risk reporting • Evaluating risk management processes • Assuring risk evaluation • Assuring risk management processes
Acceptable, but on conditions	• Facilitating identification and evaluation of risks • Coaching management in responding to risks • Coordinating ERM activities • Consolidated reporting on risks • Maintaining and developing the ERM framework • Championing establishment of ERM • Developing risk management strategy for board approval
Not acceptable	• Setting risk appetite • Imposing risk management processes • Management assurance on risks • Taking decisions on risk responses • Implementing risk responses on management's behalf • Accountability for risk management

Table 2 Internal auditor's role in ERM (adapted from IIA, 2009)

2.4.3 Implication of use of BRA approach for internal audit

Today's internal auditors are expected to identify emerging risks and help management to build an effective risk management process and strong governance. In fulfilling such newly requested demands, the internal auditors design a risk based audit plan that involves assessments of the organization's enterprise-wide risks, evaluating risk management process effectiveness, and assuring relevant controls (IIA, 2012).

As we discussed already, the internal audit functions may involve assurance and consulting services in regard to the organization's risk management process, governance, and overall internal controls placed to assure compliance, safeguarding assets, and smooth business operations. The internal audit risk assessment under BRA approach may enable the internal auditor to obtain a comprehensive evidential basis to identify ineffective corporate governance, risk management processes, and internal control systems that are more likely to adversely affect the organization.

In conclusion, both internal and external auditors are required to conduct risk assessments under the BRA approach. However, researchers find that implementing BRA is difficult due to the ambiguous linkages between business risk assessments and audit risk assessments (Knechel, 2007; Curtis and Turley, 2007; Ronson et al., 2007). Also, Knechel (2007) argues that a lack of guidance on integrating business risk assessment and audit risk assessment makes the implementation of the BRA approach more difficult (Knechel, 2007). In the following section, we discuss these obstacles to the implementation of the BRA method.

2.5 Challenges for Risk Based Audit

2.5.1 Ambiguous linkages

Researchers point out that the connections between the organization's business risks and the relevant RMM and corresponding audit procedures are not always obviously understood and are often vague (Allen et al., 2006; Curtis and Turley, 2007). Curtis and Turley (2007) find that practitioners are uncomfortable rendering an audit opinion on the client's financial statements based on indirect evidence drawn from business risk assessments and high level controls tests, rather than direct evidence from their financial reporting controls and substantive procedures. This difficulty has left the field auditor less confident with BRA and more reliant on substantive audit procedures to obtain audit evidence. (Curtis and Turley, 2007).

An organization's uncontrolled significant business risks that poses significant threats to the achievement of its objectives and goals may increase the risk of RMM, going concern issues, and other audit problems. However, the current literature lacks guidance on linking business risks to audit risk. The PCAOB (2005) also has recognized the lack of

guidance and called for more standards and guidance on effectively implementing a risk based audit practice.

Although it is difficult, linking business risk assessment, audit risk assessment, and subsequent audit procedures would be a crucially important step to successfully and effectively implement BRA. If the auditor cannot establish such links, audit risk assessment under the BRA approach would become useless.

2.5.2 Continuously changing business risks

The lack of clarification on the timing of risk assessments is another obstacle to a successful risk based audit implementation (Knechel, 2007). Although current auditing standards (e.g. the PCAOB's AS No. 12) require auditors to revise risk assessments and adjust audit plans whenever they come across new information that alters prior audit risk analysis, there is little guidance on how to recognize such new information driving changes in the audit risk assessments. Risk assessment is traditionally performed during the audit planning stage, but such a static risk assessment may not recognize dynamic shifts in the client's underlying business risks and subsequent changes in the audit risk environment.

As discussed earlier, the BRA approach requires auditors to base their audit risk analysis on the evidence from their evaluation on the veracity of the client's strategies and business processes and the effectiveness of their risk management controls to mitigate risks. Given that the client's business risks can emerge at any time during the audit, "*should the auditor take risk assessments at the end or at the beginning of the audit period*?" (Knechel, 2007). The auditor's risk assessment process should be ongoing and

dynamic so that changes in the organization's risks can be recognized in a timely manner and audit procedures can be updated in response.

Advanced information technology, globalization, and increasing use of derivative financial instruments have changed the business environment; consequently, the risk profiles an organization face may change rapidly. If such changes are not recognized and controlled in a timely manner, the organization may incur significant losses, and subsequently increased RMM. If the auditor does not address the audit implications arising from the changes in the client's significant risk profiles, they might fail to detect significant audit problems and risk audit failure.

2.6 Conclusion

Today's risk based audit practice has adopted the BRA approach which incorporates the auditor's broader understanding of an organization's strategies, objectives, related business risks, and relevant risk management control activities into audit risk analysis to determine the RMM and further audit plans.

Most major audit companies have already developed risk based audit methods which include the BRA approach and started to implement them in their audit engagements (Lemon et al., 2000; Knechel, 2007; Robson et al., 2007). Auditing standard setters have also adopted the BRA method in the current auditing standards in relation to risk assessments. These new risk assessment standards (SAS No. 104 – No. 111, AICPA, 2006c; AS5, PCAOB, 2007; PCAOB, 2010a) require auditors to understand the client's business and its environment and consider the potential impacts of business risks on RMM in conducting risk assessments and deciding the subsequent audit plans. The BRA

approach is expected to lead auditors away from traditional risk based audit practices which focus almost exclusively on the organization's business transaction cycles and relevant internal controls.

However, extant literature notes obstacles to successful implementation of the BRA approach (Knechel, 2007; Robson et al., 2007), two of which are relevant to this research. First, linking the organization's significant business risks to RMM and subsequent audit procedures is challenging for the auditor to effectively implement the BRA approach. The second obstacle is a lack of clarity and guidance on the continuous risk assessment process.

Without proper linkage, the auditor's understanding and assessment of the client's business risks and related controls would not be factored into the audit risk evaluation and further audit planning process. For an effective risk based audit practice under the BRA approach, the auditor must be able to identify significant business risks facing the client and properly link them to potential audit problems and to corresponding audit responses to address them.

Audit risk assessment is usually performed annually during the audit planning stage. This periodic and static process may not be appropriate for the BRA approach. As the organization's business environment and related risks continuously change, the auditor's audit risk assessment should be recursively and continuously carried out so that changes in the organization's risks are captured in a timely manner. Furthermore, a risk based audit plan should be adjusted in a timely manner in response to changes in an organization's significant risk profile. Therefore, risk assessment processes under the BRA approach should be dynamic and ongoing throughout the entire audit period,

continuously recognizing the organization's changing risk profile and updating audit plans in response.

Current auditing standards (PCAOB's AS No. 12 and SAS No. 109) highlight the importance of a continuous risk assessment process that allows the auditor to update risk assessments and subsequent audit plans with new information. However, current risk based audit literature does not recommend a continuous process that would facilitate keeping track of dynamic changes in the organization's risk profiles and adjusting audit plans in response to shifts in the audit risk.

As discussed in the previous chapter, our objective is to describe the key concepts of CRMA (Continuous Risk Monitoring and Assessment, Vasarhelyi et al., 2010) and propose a methodology that would provide guidance to implement such concepts. We aim to improve the original CRMA model by further developing its key concepts, definition, and methodology to offer pragmatic guidance to build a continuous risk assessment and dynamic audit planning process.

CRMA is a new CA (continuous assurance) procedure that allows the auditor to continuously monitor the organization's enterprise-wide risks, identify uncontrolled risks (i.e., significant business risks), and prioritize the corresponding audit and risk management procedures which address those high exposure risks in an ongoing manner. CRMA is consistent with the BRA approach. CRMA procedure may enable the risk based auditor to design and implement a continuous risk assessment in conjunction with the BRA approach.

The proposed CRMA methodology suggests a mechanism to monitor and assess the organization's risks in a continuous manner and link them to relevant audit procedures (as well as risk management procedures to be performed by management) in response to the organization's current risks profile. Development of CRMA methodology as a new component of CA procedure not only contributes to the CA literature, but also fills a gap in the risk based audit literature.

In chapter 3, we discuss CRMA in more detail; we present its background, key concepts and rationales, and our methodology to develop CRMA procedures.

Chapter 3: CRMA Methodology for Continuous Risk Assessment and Dynamic Audit Planning Process

3.1 Introduction

Vasarhelyi et al. (2010) originally propose CRMA (Continuous Risk Monitoring and Assessment) as a new type of CA (Continuous Assurance) procedure for a risk based system. They envisage using CRMA to turn CA into a risk based dynamic system that would more effectively deal with the changing business and audit environment, and they call for more research on CRMA. In response, we propose a methodology to build a CRMA procedure. In this chapter, we describe the key concepts and background of CRMA, and propose a methodology for CRMA development.

The proposed methodology for continuous risk assessments and dynamic audit planning may offer a new approach to evaluating and understanding the organization's dynamic risks and the effectiveness of its risk management controls in the conduct of the risk based audit with the BRA method. Furthermore, the continuous audit and risk management procedures adopted in the proposed CRMA methodology may enable the BRA auditor to link the organization's uncontrolled significant risks to corresponding audit procedures in a consistent and timelier manner.

In the remainder of this chapter, we first provide the background of CA and the extant methodologies to build its applications, such as CDA (Continuous Data Assurance, Alles et al., 2008) or CCM (Continuous Control Monitoring, Alles et al. 2008). We next discuss the evolution of CRMA as a new CA methodology and detail a CRMA methodology.

3.2 Continuous Assurance (CA)

Since its first pilot study by Vasarhelyi and Halper (1991), CA[16] has gained wide recognition for enhancing corporate governance and real-time operation controls (Chiu et al., 2013). In 1999 the joint committee of the AICPA and the CICA issued a research report on CA (CICA/AICPA, 1999) and define it as

"[A] methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity's management is responsible, using a series of auditors' reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter" (AICPA/CICA, 1999).

Since this joint report, CA has been more widely recognized, implemented, and studied by both practitioners and academics (Alles et al., 2008; Chiu et al., 2013).

In principle, CA utilizes real-time monitoring and processing technologies to continuously monitor and analyze business process data and execute certain automated audit procedures to detect errors or exceptions which could result in material audit problems (Vasarhelyi et al., 2004). While the traditional manual audit is performed annually and relies on sampling techniques and statistical inferences, CA procedures could run year-round and examine the entire population of the audit targets, providing audit results almost immediately after underlying auditable events occur.

---

[16] The literature often uses the terms Continuous Auditing and Continuous Assurance interchangeably, although they have slightly different meanings (Alles et al., 2002). The former deals with the standard attestation audit procedures such as financial statement audits or audits for internal control (Alles et al., 2002), whereas the latter encompasses not only the attestation based audits, but also consulting based services for other subjects that goes beyond the traditional attestation areas such as risk assessment, business performance measurement, information systems reliability, etc. Since CRMA methodology encompasses the prioritization of risk management audit procedures which is beyond the scope of traditional auditing services, the term Continuous Assurance would be more suitable for CRMA methodology. Therefore, in this paper CA refers to Continuous Assurance.

CA is conceived as the future model of auditing in the 'real time economy' where advanced IT systems and Internet based networks process business transactions and communicate their results in real time (Rezaee et al., 2001; Elliot, 2002; Vasarhelyi et al. 2004; Alles et al., 2008). Alles at al. (2006) assert that CA is an outcome of today's prevalent use of automated and integrated information systems. They view that the demand for CA has increased as more companies use real-time IT or integrated ERP systems to automate their business processes, integrate information flow, communicate with users in real time, and desire to assure such real-time generated information (Alles et al., 2006).

The benefits of CA have been acknowledged worldwide. KPMG's survey (2012) which examines the awareness about and the current and future status of CA find that many organizations in Europe, Middle East, and Africa are aware of the benefits of CA technology. The survey finds that the majority of respondents expect that CA would bring comprehensive assurance with grater coverage across the organization (89%). A majority also believes that CA will facilitate real-time operational assurance (81%) and reduce the burden for line management (74%) (KPMG, 2012).

3.2.1 Structure of CA

Kogan et al. (1999) explain that a CA system would ideally work out on two conditions: (1) a fully automated process and (2) a process with instant access to relevant events and their outcomes (Kogan et al., 1999). CA is built on and takes advantage of the organization's integrated and automated business processing systems in conducting audit tests in a real time and automatic manner. Automated and real time audit procedures could examine underlying transactions as they occur, enabling continuous auditing. Such

an application could be embedded in or loosely connected to the organization's information systems, analyzing its transactions and identifying anomalies.

Since the 1990s the widespread adoption of ERP (Enterprise Resource Planning) systems with centralized database management has provided highly integrated and automated technology foundations and a common data base for the implementation of CA (Debreceny et al., 2005). ERP applications integrate diverse business processes such as sales and customer service, purchasing, inventory management and logistics, and accounting, meaning data entered by one department could be re-used for other business processes without requiring re-entry. With centralized database management systems and unified data, ERP applications integrate functionally different business processes and streamline data flow. CA procedures are enabled by such information systems to examine the organization's transactions in a short time cycle or in real time. The following section discusses two common structures that allow CA.

3.2.1.1 Embedded Audit Modules (EAM, Groomer and Murthy, 1989)

EAMs are Computer Assisted Audit Tools and Techniques (CAATTs) that enable continuous monitoring of the organization's financial reporting systems. EAMs are embedded in the organization's real time information systems, continuously monitor the flows of transactions, detect abnormal transactions, and alert the auditor once any violation or exception is detected (Debreceny et al., 2005, Kuhn and Sutton, 2010). EAMs are considered an important IT structure needed for the adoption of CA (Alles et al., 2002; Kogan et al., 1999; Vasarhelyi and Halper, 2002).

Groomer and Murthy (1989) initially propose using an EAM (Embedded Audit Module) to monitor and detect auditable problems with the organization's database controls and

security. They argue that EAMs could potentially capture 100% of transaction errors and control violations, improving assurance on integrity of the organization's database driven accounting information systems.

However, the use of EAMs involves several drawbacks (Groomer and Murthy, 1989, p. 68). First, the auditor must have some IT knowledge to effectively implement and manage EAMs. Second, the auditor needs cooperation from the auditee in implementing EAMs into their database systems. Third, the auditee's system should be stable, not vulnerable or expected to be modified often. An unstable system would require EAMs to be updated or modified often, increasing the cost of EAMs significantly. Debreceny et al. (2003) document possible limitations in developing and utilizing EAMs in an e-commerce environment by simulating 10 EAM examples.

3.2.1.2 Monitoring and Control (MC) Layer (Vasarhelyi and Halper, 1991)

While EAMs may be understood as CA modules embedded in the organization's systems, the monitoring and control (MC) layer is an intermediary architecture which connects the CA system and the organization's systems (Vasarhelyi et al., 2004; Kuhn and Sutton, 2010). Along with EAMs, the MC layer plays an important role in analyzing transactions and data flow and detecting audit significance in a continuous manner.

The MC layer is an overlay of analytic control processes on top of a monitoring architecture in a CA system (Vasarhelyi et al., 2004). MC is used to probe the organization's real time systems, extract, and analyze real time process data to identify exceptional transactions. The difference between MC and EAMs is that the former could be used for organizations that lack highly integrated and automated systems; the MC layer may be designed to extract the data from the organization's legacy systems,

different non-compatible applications, or externally linked web-facing systems and analyze the collected data for exceptional cases in a continuous manner.

Vasarhelyi and Halper (1991) tested MC in a real business environment at Bell Laboratories (Alles et al., 2008). They implemented an outlay of analytical modules, referred as Continuous Process Auditing Systems (CPAS), to monitor and control processes used in AT&T's real-time billing systems. CPAS ensures system integrity in real time through automated data acquisition, analysis, and alarm alerts triggered when erroneous data are detected in the billing systems. Based on CPAS implementation, they explain how an automated audit module monitors process controls, detects erroneous data, and reports to the auditor immediately through alarms, facilitating a real time assurance.

The MC layer carries out two key functions of CA: (1) data gathering and (2) monitoring and analysis. The analytic monitoring activities of CA distinguish it from the traditional audit. Analytic monitoring would observe events as they occur, send an alarm when exceptions or discrepancies occur, drill down to fundamental sources of the exceptions or discrepancies, integrate data across the organization's different systems and processes, and automate audit tests (Vasarhelyi et al. 2004).

Such analytic monitoring functions enable a closer-to-the-event audit review and distinguish CA from the traditional 'ex post' review (Vasarhelyi et al., 2004). Like EAMs, the MC layer monitors the flows of the organization's transactions and detect the exceptions, unprecedented unusual events, or controls violations based on the auditor defined heuristic rules (Vasarhelyi et al., 2004).

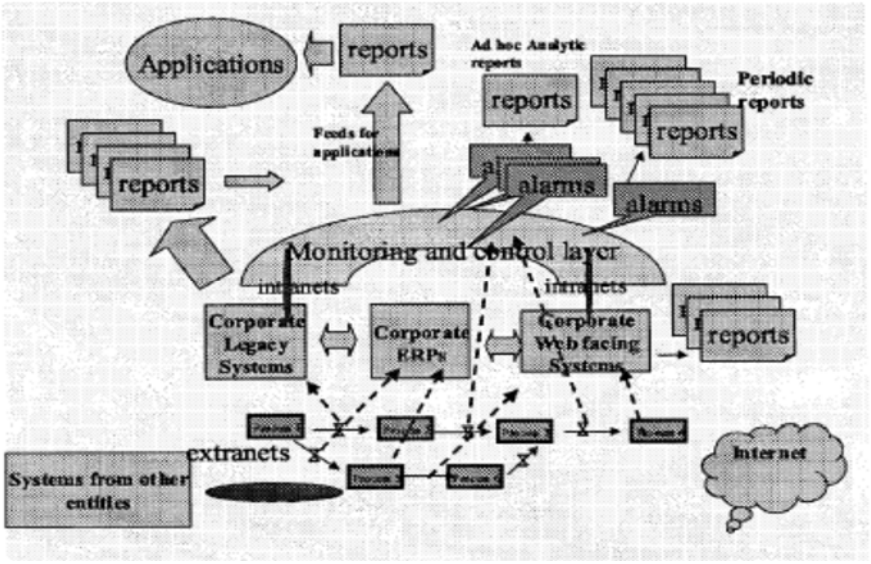

Figure 3 Monitoring and Control Layer (Excerpted from Vasarhelyi et al., 2004)

Rezaee et al. (2002) also view that effective development of a CA system requires creating an IT structure for accessing and extracting data from different legacy systems and platforms. They propose building an audit data warehouse and audit data mart to acquire the organization's underlying transactional data and automate audit testing in a continuous manner. They envisage that CA's capacity to monitor the organization's transactions and identify the audit significances would be improved by using audit data marts and warehouses fed by the organization's main database on an ongoing basis.

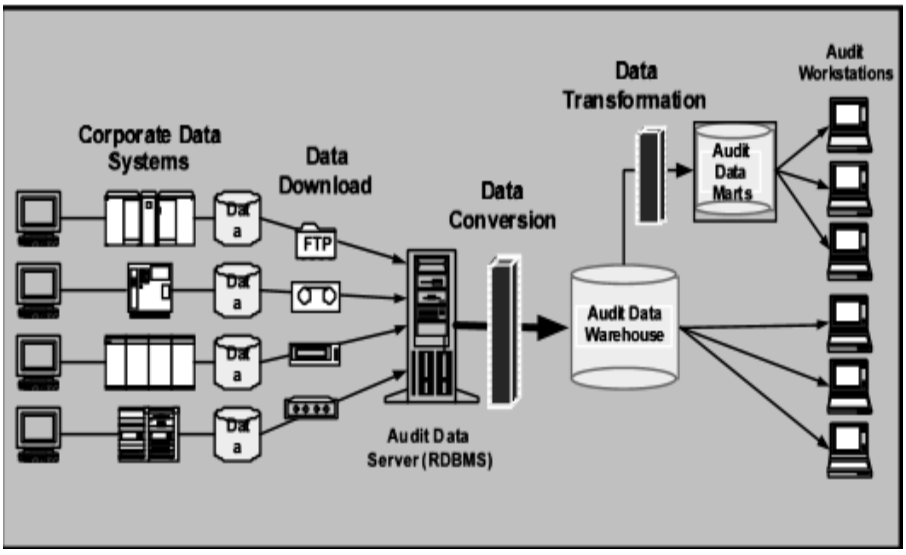

Figure 4 Continuous auditing using audit data warehouse (excerpted from Rezaee et al., 2002)

3.2.2. Components of CA: CDA, CCM, and CRMA

Alles et al. (2008) view that a CA system can be designed and implemented either to test internal controls (Continuous Control Monitoring (CCM)) or to carry out substantive tests (Continuous Data Assurance (CDA)) or both. CDA continuously detects and reports material errors in the entity's transaction data stream, and is thus used for substantive testing purposes including analytical procedures. CCM focuses on monitoring and recognizing internal control violations in a real time manner, facilitating internal control testing. CDA and CCM continuously monitor and analyze transactional data and control processes and provide the auditor with immediate feedback as soon as material errors or control violations are detected.

Continuous Assurance = Continuous Data Assurance (CDA) + Continuous Control Monitoring (CCM)

Different procedures and approaches for CDA or CCM may be needed for organizations with different business processes. Along with CRMA which will be presented in the later,

CDA and CCM would provide conceptual models and basis to identify the objectives of CA applications and develop appropriate CA procedures achieving given CA objectives. That is, depending on which procedure is used among CDA, CCM, or CRMA, a CA application may be designed for detecting data anomalies, control violations in the organization's particular business processes or transactions, or emerging significant risks in particular organizational areas of the organization, respectively.

3.2.2.1 Continuous Data Auditing (CDA)

CDA continuously analyzes the organization's transaction data and identifies erroneous data or exceptions which are indicated by discrepancies between the actual and expected values or benchmarks, facilitating analytical procedures at the substantive testing level. CDA filters out exceptional transaction data that violates business process rules at the transaction, disaggregated. Kogan et al. (2007) argue that under most circumstances the real time data analysis to detect data errors works best with disaggregated data. CDA would perform effective substantive tests for financial statement assertions by examining disaggregated transaction data.

Kogan et al (2007) propose to use 'business process audit benchmarks', or 'Continuity Equations', to identify anomalies in transactional data flows. They define continuity equations as "*stable probabilistic models of highly disaggregated business processes*", or expectation models that predict values and identify anomalies that differ significantly from the predicted values. They suggest three probabilistic models as candidates for the continuity equation benchmarks: Simultaneous Equation Model, Vector Autoregressive Model, and Linear Regression Model. CA can use these procedures to continuously and automatically detect anomalous transaction data (disaggregated data) before they are

aggregated and result in material errors in the financial reports. Alles et al. (2008) demonstrate the use of highly disaggregated data in testing audit evidence about the integrity of a large health service provider's supply chain process by using its procurement transaction cycle data.

3.2.2.2 Continuous Control Monitoring (CCM)

CCM is the set of CA procedures that allows for the continuous monitoring of internal controls of business process (Alles et al., 2008). CCM is often driven by management needs for improving their internal controls to comply with Sarbanes-Oxley requirements. This is consistent with the concept that Continuous Monitoring (CM) is defined as a management driven activity, while CA is audit driven (Warren and Parker, 2003).

CCM monitors system controls and detects significant control violations that warrant auditor's close investigations for further audit procedures. As CCM continuously monitors control effectiveness and detects control failures or violations, it enhances the efficiency and effectiveness of compliance audits. For example, CCM can be designed to audit the IT system security controls by automating audit procedures to examine the effectiveness of IT security controls. Automated audit procedures by CCM can continuously monitor and check IT systems and detect suspicious activities or transactions that could threaten IT security. Automated audit procedures within CCM running in continuous manner will save time and labor when compared with manual procedures, allowing auditors to spend more time on audit judgments.

Alles et al. (2006) report on an implementation of CA at Siemens Corporation. Their CA application would be on top of Siemens' SAP R/3 system to continuously monitor the business process controls, making it an application of CCM. In their CCM model, data

was extracted in batch mode from the Siemens SAP system and formalized, thus automatable audit procedures were designed for business process controls testing. The authors emphasize that formalization of audit procedures is necessary to build a CA system, indicating a certain level of necessary audit process reengineering with a focus on replacing non-formalizable audit procedures with formalizable equivalents.

3.2.2.3 Continuous Risk Monitoring and Assessment (CRMA)

Vasarhelyi et al. (2010) first introduce CRMA as a new CA procedure that continuously monitors and assesses the organization's risks and prioritizes subsequent audit procedures in response to changes in the organization's risk profile. They stress that the development of CRMA is necessary to keep a CA system agile and robust. They point out that today's CA system should be capable of assessing the organization's risks on an ongoing manner as many modern organizations use real-time IT systems and employ enterprise-wide risk management processes, such as ERM, which would enrich the data environment for a CA program to retrieve and monitor relevant risk related data and metrics to assess the organization's risk exposure levels in a real time manner. In 'Continuous Assurance for the Now Economy', they define the ultimate objective of CRMA:

"The aim of CRMA is to give Continuous Assurance systems robustness to deal with shocks to the audit environment and thereby to make the Continuous Assurance system dynamic rather than static" (Vasarhelyi et al. 2010, p54)

3.2.2.3.1 CRMA Framework

As shown in Figure 5, CRMA is described as a risk assessment framework that takes the organization's various risks, computes their significance levels to the organization, and arranges and prioritizes audit and risk management procedures to mitigate the organization's highest risk exposures and related RMM (risks of material misstatement),

enabled by algorithmic formal procedures so that such risk assessment process can be executed automatically and continuously. CRMA is expected to provide ongoing risk assessment and make CA more dynamic.

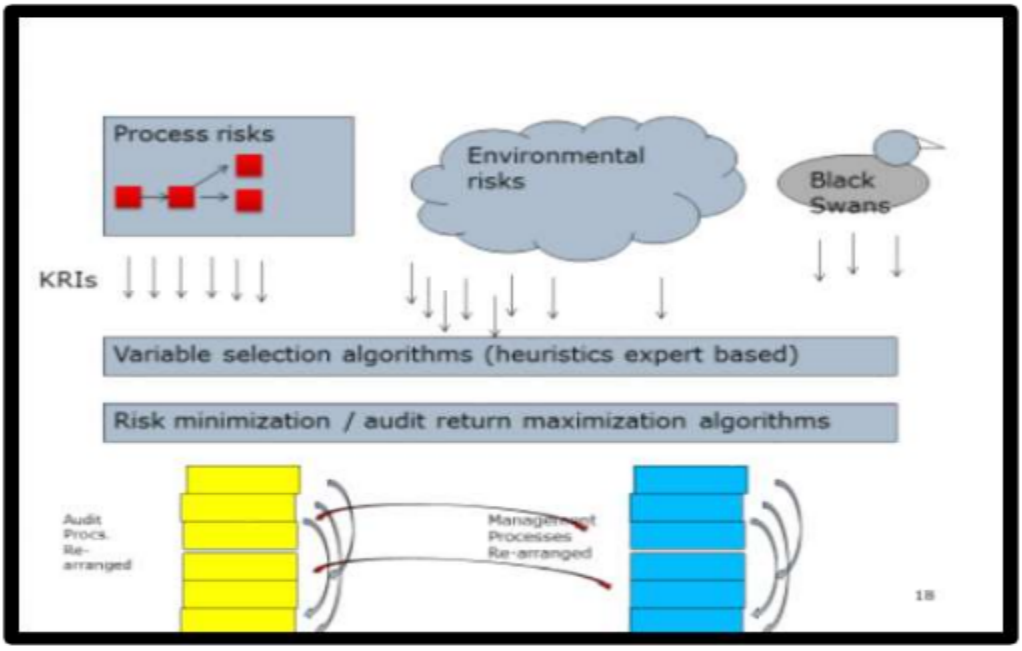

Figure 5 CRMA framework (Bumgarner and Vasarhelyi, 2014)

As shown in Figure 6, CRMA is depicted as a risk assessment model that takes all available information (internal and external sources) and provides the results of its risk assessments to other ongoing CA procedural components such as CDA and CCM in a continuous manner.

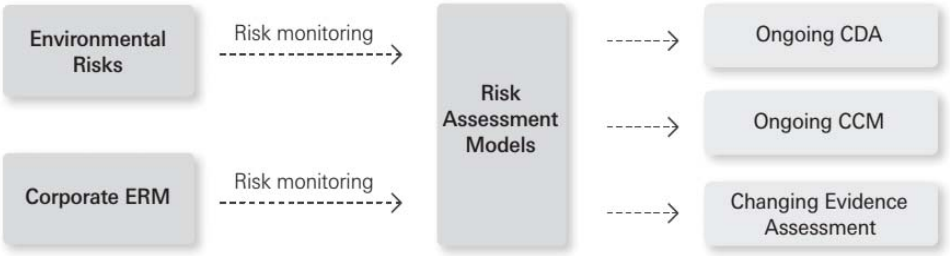

Figure 6 CDA, CCM, and CRMA (Vasarhelyi et al. 2010, p56)

CRMA can complement CDA and CCM by continuously prioritizing audit procedures according to changes in the organization's high level risks.[17] From this perspective, Vasarhelyi et al. (2010) describes CRMA, CDA and CCM as distinct, but complementary components of a risk driven CA system as shown in Figure 7.

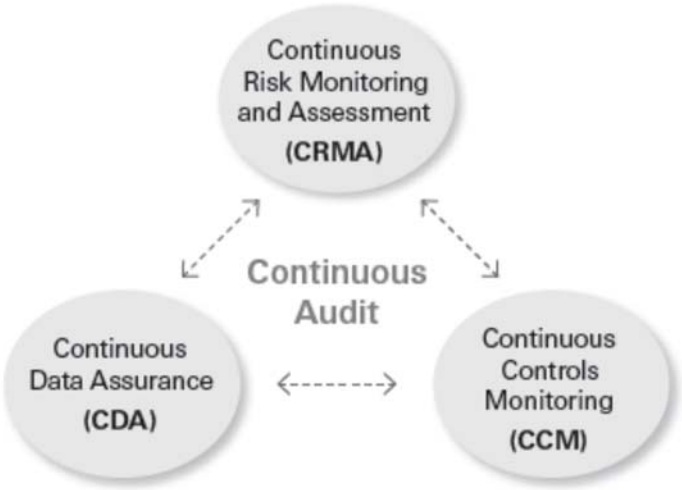

Figure 7 Three Elements of CA (excerpted from Vasarhelyi et al., 2010, p 41)

3.2.2.3.2 Definition of CRMA

Based on these original conceptions of CRMA and its framework model described by Vasarhelyi et al. (2010), we formally define CRMA as *a CA procedure that enables*

[17] A static CA system would not respond to change in the organization's risk profiles, but apply its procedures on the same target continuously.

continuous risk assessment and dynamic audit planning processes that monitor and assess the organization's risk exposure levels in real time and prioritize subsequent audit and risk management procedures.

This ongoing risk assessment and dynamic audit planning process is the essential aspect of CRMA and characterizes the role of a CRMA procedure in the risk driven CA system.

3.3 CRMA Methodology

We propose a novel methodology to build a CRMA procedure and explain our theoretical basis for the proposed methodology throughout this chapter. We establish key concepts and a theoretical framework to identify and assess the organization's risks, steps and methods to monitor and quantify them in order to consistently prioritize subsequent audit and risk management procedures. The proposed methodology for CRMA is drawn from the original CRMA framework proposed by Vasarhelyi et al. (2010) as shown in Figure 8.

The proposed CRMA methodology consists of four steps: (1) identification and selections of the organization's risks to be monitored, (2) identification and selection of KRIs (Key Risk Indicators, IOR, 2010) for those selected risks, (3) monitoring and assessment of selected KRIs for each given risk and its exposure level, and (4) prioritizing subsequent audit and risk management procedures according to the organization's high exposure risks.

In the following section, we provide the key concepts, assumptions, and methodological procedures required in each step of the proposed CRMA methodology.

CRMA Methodology (4 steps)

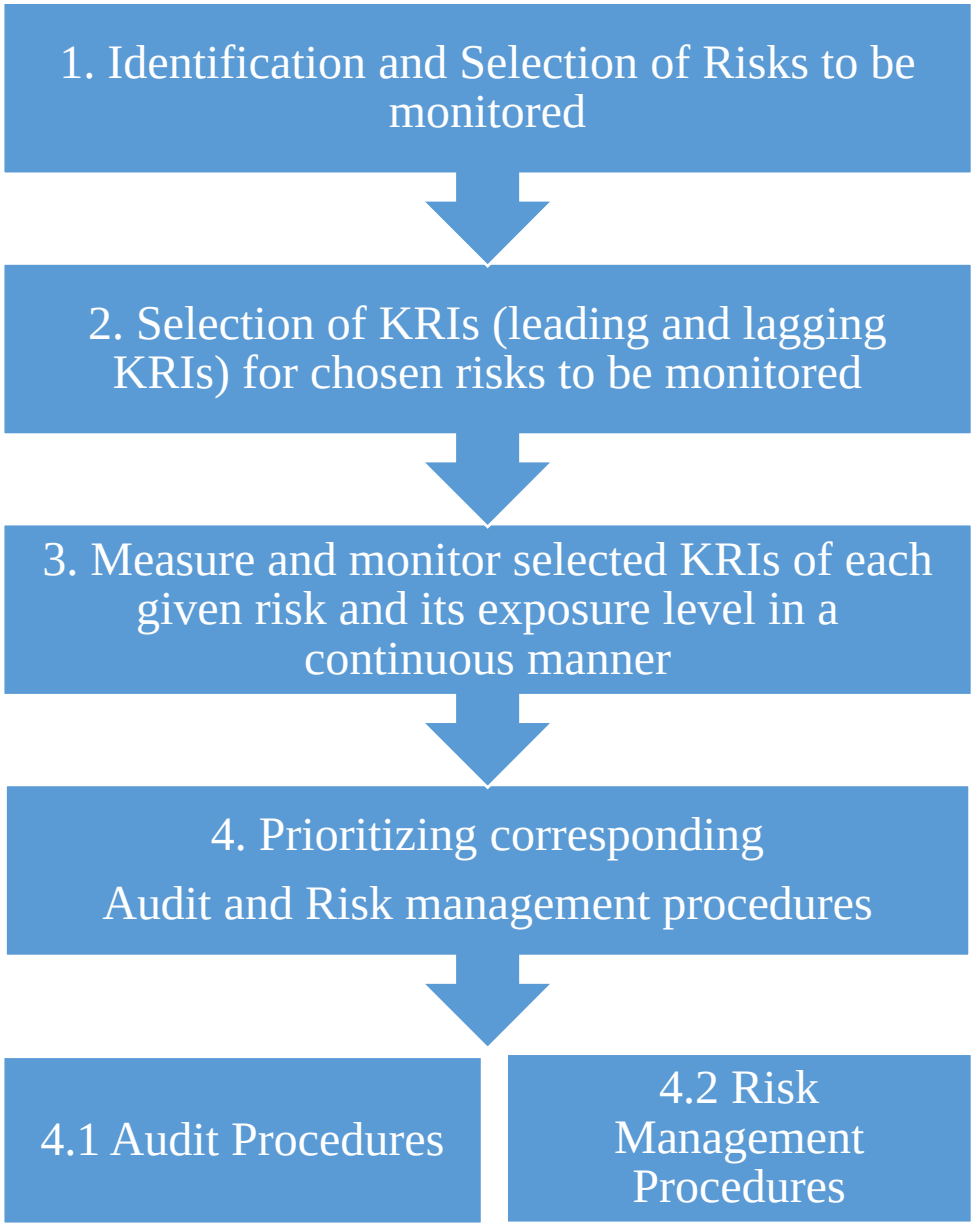

Figure 8 Four steps of the proposed CRMA methodology

3.3.1 Step 1: Identification and Selection of Risks to be monitored

3.3.1.1 Risk Categories in CRMA

The proposed CRMA methodology involves identification and assessment of the organization's significant uncontrolled risks and prioritizing subsequent audit and risk management procedures. To begin the process, the proposed CRMA methodology requires the auditor to identify risks to be monitored after the careful consideration of all potential risks that may significantly affect the organization's strategic objectives.

The proposed CRMA methodology suggests using three risk categories: (1) Process risk, (2) Environmental risk, and (3) Black Swans (Taleb, 2010) (Figure 9).

Figure 9 CRMA Risk Categories

Process risks may include all probable adverse events stemming from inefficient internal processes, including management or employee fraud, accidents or injuries, inefficient departmental functions or strategic initiatives such as HR, finance, supply chain management, customer relation management, enterprise risk management, etc. (Miller, 1992; Robert, 2006)

Environmental risks include all possible events that are largely caused by the organization's external forces. Such risks may include political turmoil, government

regulations or sanctions, macroeconomic uncertainties, market uncertainties, enhanced competitions, changes in the customer's preferences, changes in creditworthiness of third-party customers or partners, natural or hazard uncertainties, etc. (Miller, 1992).

Black Swans are events that are not usually observed in the past and therefore cannot be predicted from historical data, and are only explained after the fact as outliers (Taleb et al., 2009, Taleb, 2010; Nafday, 2011). Black Swan events are normally characterized as unknown unknowable, as they are unthinkable before the fact. Examples of Black Swans[18] include the 9/11 terrorist attack, the 9.0 earthquakes and subsequent tsunami that caused nuclear reactor failures in March, 2011 in Japan, the explosion of the Columbia shuttle in 2003, and the breakout H1N1 flu in 2009 (Pate-Cornell, 2012).

While increased complexity and globalization have increased the likelihood of a Black Swan (Taleb et al., 2009), they may not be estimated convincingly by traditional probabilistic risk analyses which depend on past historical data. Taleb et al. (2009) argue that a better way to deal with Black Swans is to reduce the vulnerability of the organization in case they occur.

However, some researchers argue that the organization could more effectively deal with Black Swans by utilizing a more proactive risk management approach that promotes risk awareness, quick detection, and early response (Aven, 2013; Pate-Cornell, 2012). Pate-Cornell (2012) assert that although Black Swans are unknown a priori, their development could be possibly imagined through careful observation and analyzing early signals

[18] Black Swan is often compared to Perfect Storm; former represents the ultimate 'epistemic' uncertainty in which the underlying event is not known before and unknowable (unknown unknowable), but latter involve 'aleatory' uncertainties where the underlying event is known, but very rare to observe which is referred as unknown knowable (Pate-Cornell, 2012).

indicating their emergences[19]. Nafday (2009) also suggests that the organization's managers should think through potentially harmful consequences which may occur (with a mind that "absence of evidence is not evidence of absence") and develop certain tactics or strategies to deal with such potential consequences of unforeseen Black Swan events.

3.3.1.1.1 Assessments of Black Swans

The proposed CRMA methodology proactively identifies, assesses, and manages Black Swan events. The proposed CRMA methodology utilizes more real-time data to monitor and recognize the signals of emergence of the organization's black swan events.

To monitor and assess an organization's black swan risk, the CRMA auditor should brainstorm imaginary black swan events first by reasonably imagining rare and unknown events in the past that could significantly affect the achievement of the organization's objectives and goals. The proposed CRMA methodology considers black swan events in a different frame in order to identify and quantify them; in the proposed CRMA methodology, black swans are defined as very rarest, unknown, and unknowable because they never observed before, but imaginable through 'reasoned imagination' (Pate-Cornell, 2012). With regard to the identification of black swan events, Pate-Cornell (2012) argue:

"Obviously, the truly unimaginable cannot be envisioned upfront, but signals (for instance, medical alerts that a new virus has appeared, or new intelligence information) can be observed, suddenly or gradually. Reasoned imagination is thus an important part of risk assessment because it implies, first, anticipating by systematic analysis scenarios that have not happened yet, and second, recognizing and communicating these unusual signals" (p. 1825).

[19] Some Black Swan events are arguably imaginable if the similar, but not exact events observed in the past. An example is 9-11 attack. Similar airplane hijackings attempting at attacks occurred in the past (Pate-Cornell, 2012).

Some examples of possible black swan events for the organization may include cyber-attacks that damage the organization's entire servers including backups in an unexpected way, unusual floods or hurricanes in certain area resulting in losing the large customer bases or suppliers, collusion of trusted senior managers who trade the organization's secrets (such as Coca-Cola formula), earthquakes in normally safe operational locations, or high ranked officers' inappropriate actions that could damage the organization's reputation (such as the 'nut rage' incident with Korean Airline, The New York Times, 2014).

Once such black swan events are identified through reasonable imagination, the next step is to select all relevant leading or lagging KRIs[20] (Key Risk Indicators, IOR, 2010) of the identified black swan events. Then, such selected KRIs would be monitored and combined to quantify the given black swan risk exposure levels in a continuous manner[21].

Black swans could occur at any time and damage the organization. The risk based auditors would need to examine how the organization manages its potential black swan events. If not, the achievement of the organization's strategic objectives and intended performance targets may fail once the black swan events occur. Thus, for the risk based auditor, it would be important to examine how the organization effectively deals with the black swan events to assure the achievement of its objectives and desired performance levels. However, extant literature does not address how to treat the risk of black swan damage when assessing the organization's risks and determining audit risk and further

[20] KRI (Key Risk Indicator) is a data or metric that indicates the status of a given risk (whether it is rising, remote, or materialized). Any type of data could be a KRI as long as it represents the given risk's exposure level (Hwang, 2010; ISO, 2010)

[21] Such continuous risk assessment and monitoring procedures using KRIs proposed as a CRMA methodology will be further explained later in this chapter.

audit plans. The present study is the first that addresses black swans in the context of a risk based audit. Continuous monitoring and assessments of relevant KRIs of imagined black swans supported in the proposed CRMA methodology would facilitate the recognition of emerging black swans in the organization and prompt audit responses to address the affected audit risk.

3.3.1.2 Selecting the organization's risks to be monitored

Once the risks that could significantly affect the achievement of the organization's strategic objectives and goals are identified, the next step in the proposed CRMA methodology is to determine which of these risks will be monitored. The organization's risks that are expected to have the largest impact may be selected for continuous exposure level monitoring (Davies et al., 2006; Grabowska et al., 2007; Scandizzo, 2005). To stratify risk impact, the CA auditor should consult with the responsible management or risk manager to understand which risks are conceived as the greatest threats for them.

3.3.2 Step 2: Develop KRIs for each selected risk to be monitored.

Once the risks to be monitored are selected, the next step is to select relevant KRIs to monitor the organization's exposure to those selected risks and rank them by exposure level. In general, a KRI is defined as data or metric to monitor the level of risk exposure overtime (Davies et al., 2006; IOR, 2010; Hwang, 2010). Any type of data that could present the current status of the risk (rising or remote) may be considered a risk indicator (IOR, 2010). In the next sections we provide the rationale for using KRIs, the framework to select relevant KRIs, and the methods to evaluate and integrate observed KRIs' values to quantify the organization's risk exposure.

3.3.2.1 Use of real time data

Vasarhelyi et al. (2010) point out that it is necessary to have a more realistic measurement of the organization's risks and lessen reliance on past data in order to make audit risk assessment more robust. Conventional probabilistic models and methods relying on historical patterns may not anticipate the future when the organization's business environments change rapidly. The likelihood of a given risk today may not be as same as one measured last week. Relying on the standard probability distribution or historical frequency distribution may not reflect changes incurred in the current business environment, hindering accuracy.

Utilization of more current information about the organization's business processes and operations may be more effective in assessing the organization's risk exposure levels, especially when their business environment changes rapidly. The proposed CRMA methodology utilizes KRIs which could provide more current or real-time information about the organization's business processes and operations to better recognize the organization's significant risks in a timelier manner.

As a CA procedure, CRMA takes advantage of the organization's integrated and automated IT structure to continuously monitor current business operations data and performance metrics. With aid of such automated and integrated IT systems, the continuous data monitoring and analytics part of the given CA system would be able to monitor current business process data, including enterprise-wide risk management process data and performance metrics, in real time. The proposed CRMA methodology focuses on monitoring and measuring relevant KRIs and assessing exposure levels in real-time.

3.3.2.2 Key Risk Indicators (KRIs)

"A KRI is a measure to indicate the potential presence, level, or trend of a risk. A KRI is first and foremost a measurement tool. It can indicate whether a risk has occurred or is emerging, a sense of the level of the risk exposure, the trending of and / or changes in risk exposure" (Hwang, 2010)

In general, a KRI is any type of data or metric that provides information about the status of a given risk. KRIs may provide insight into risk development or exposure by representing the symptoms of its presence and severity (Davies et al., 2006; IOR, 2010; Hwang, 2010).

The Institute of Operational Risk (IOR, 2010) argues that a good KRI should be relevant, measurable, predictive, easy to monitor, auditable, and comparable. For example, volume of unresolved customer complaints could be an operational risk KRI. Customer satisfaction is vital for successful business operations and minimization of operational losses. Unsatisfied customers may bring product returns, bad reputation, or even lawsuits, portending significant losses and increasing the organization's operational risk exposure level. An increase in the number of unresolved customer complaints could be a symptom of rising operational risk exposure. Complaint data may be measured by analyzing related business process records such as call center log books or customer surveys. By monitoring complaint trends, the organization may predict the likelihood of operational losses from unsatisfied customers. Thus, the number of unresolved customers' complaints is relevant, measurable, and predictive for assessing operational risk exposure. Some other examples of KRIs include staff turnover, the number of accidents, and the number of virus or phishing attacks (IOR, 2010).

Quality KRIs could provide early warning signals that allow for more proactive risk response strategies and remedial actions (Hwang, 2010). Monitoring KRIs would keep management continuously apprised of emerging risks and help them to act quickly to mitigate those emerging risks. KRIs could work as triggers to initiate risk response actions or early warning systems to alert the first signs of trouble (Matz, 2008).

Trends in KRIs would provide useful information to evaluate whether the organization's exposure to a particular risk is increasing or decreasing (Hwang, 2010). KRIs that breach pre-assigned thresholds or limits may signal significant changes in risk. KRIs are often used to report risk profile information to senior management, anticipate emergence of major risks, manage and integrate the risk management efforts, and promote risk awareness and day-to-day management of routine risks (Davises et al., 2006).

A survey conducted by Risk Management Association (RMA) in 2011[22] reports that the top four reasons for using KRIs are risk and control self-assessment (RCSA), board reporting, scenario analysis, and capital modeling. The survey also shows that KRIs are used both at the corporate level and the business unit level. 67% of the survey respondents use KRIs and 28% are in the KRI program development process, indicating 95% of respondents value KRIs. 41% of KRI users have 1 to 25 KRIs, 12% have 26 to 50, another 12% have 51 to 70, 6% have 76 to 100 KRIs, and 24% have more than 100 KRIs (RMA, 2011).

3.3.2.2.1 KRI and KPI

KRI and KPI (Key Performance Indicator) are both metrics, while KRIs monitor risk exposure, KPIs monitor performance targets (IOR, 2010; Hwang, 2010; Beaseley et al.,

[22] The survey is based on interviews with 18 financial institutions (RMA, 2011)

2010). KPIs measure actual performance on a wide range of strategic, tactical, and operational objectives, such as revenue or profitability, market share, and customer satisfaction, thus they are 'lagging' in nature (Hwang, 2010).

A KPI may be also used for a KRI as long as it provide information to anticipate a potential risk event increasing the organization's risk exposures (Beaseley et al., 2010). For example, the number of defective products returned could be a KPI for the product production process, but it may be also used as a leading KRI for the organization's operational risk (i.e., losing loyal customers, product recalls, etc.). However, not all KRIs are KPIs. For example, the percentage of staff taking no vacation could be a KRI that offers information to have insight into the likelihood of potential fraud occurring, but not a KPI (Hwang, 2010).

3.3.2.2.2 Early Warning Signals

Relevant literature supports the use of KRIs for exposure monitoring and detection of early signals. For example, Matz (2008) suggests the use of early warning KRIs to better manage liquidity risk at financial institutions. Scandizzo (2005), IRO (2010), Sundmacher and Ford (2004) and Davis et al. (2006) suggest using KRIs or KRI composites to monitor and improve operational risk management initiatives. Beasley et al. (2010) propose utilizing KRIs to monitor potential changes in the organization's risk environment. Hwang (2010) also advocates the application of KRIs to facilitate monitoring the organization's risk exposure levels and complement other risk management tools for an effective integrated risk management process, such as ERM. Grabowski et al. (2007) propose an approach to identifying and validating leading KRIs

of safety for the marine transportation industry. Øien et al. (2011) developed early warning KRIs to reduce the risk of fatal accidents in the chemical industry.

3.3.2.2.3 Leading indicators: Near misses or precursors

The term ‘near-misses’ refers to the events that did not cause damage, but had very high chance of doing so[23] (Seki and Yamazaki 2006; Rosenthal et al. 2005; Barger et al. 2005; Phimister et al. 2003; Kaplan 1990; Paté-Cornell 2004). Some researchers propose to use of near-misses data to improve an organization’s process safety and product quality (Pariyani et al., 2011) Pariyani et al. (2011) propose a methodology to evaluate the level of safety and product risk at chemical facilities, which utilizes ‘near misses’ data from the distributed control and emergency shutdown systems, rather than using the databases of actual accidents, to calculate the probabilities of system failure and accidents.

‘Near-misses’ may represent precursors to a larger problem (Pariyani et al., 2011). While there may not be a causal relationship between precursor information and the risk event, correlation alone provides valuable risk prediction information (Pariyani et al., 2011). Such near-misses or precursors information may be used as leading indicators to anticipate an organization’s potential risk events. For example, the selling defective cars to dealerships is an important risk to be managed at a luxury car manufacturer. The event of selling defective cars may coincide with the unexpected disruptions in the manufacturer’s supply chain management process, such as delayed delivery or poor quality parts, strong competitions in lowering costs among the suppliers, frequent breakdowns of factory machines, increasing rates of inspection failure, etc. These events would be precursors or near-misses to the selling of defective cars to customers.

[23] Some researchers define ‘near-misses’ as almost happened events (Dixon and Schreiber, 2011)

Although these near-misses events may not always cause the selling of defective cars to customers, their frequent observance may indicate the risk of selling defective cars is arising. Therefore, the presence of precursors or near-misses events may be considered as leading KRIs that represent the signals of rising risks in the organization.

In a risk based audit context, assume that the internal auditor keeps track of such precursor or near-misses information as leading indicators for the risk of selling defective cars to the customers by understanding and monitoring the organization's supply chain processes efficiency on an ongoing basis. Then, they would be able to better recognize the changes in the risk level timely manner, thus more likely to mitigate the potential problems caused by the risk, such as inefficient production and inspection process controls, more customer disputes, possible litigation loss, etc. On the contrary, assume that the internal auditor relies on past performance data, such as last month's KPIs (number of recalls, inspection report, customer surveys etc.) to assess the risk of selling defective cars to the customers to plan their risk based audit for the current year. Then, they would not be able to detect the changes in the risk level that may occur during the current period and may result in inaccurate risk assessments and inefficient risk based audit planning.

As precursor information indicates the situations or circumstances before the underlying risk events occur, by tracking it, the risk based auditor would be better able to sense emerging risks in a timely manner. The proposed CRMA methodology takes such 'near-misses' and precursors as leading indicators to measure the organization's exposure level to a given risk.

3.3.2.2.4 Confirmatory Event Indicators (CEI): Confirming risk events

As well as leading indicators, the proposed CRMA methodology uses indicators that represent the status or situation appeared once a given risk has occurred in assessing its current risk exposure level in an organization. We call such indicators as Confirmatory Event Indicators (CEIs). While leading indicators are used to anticipate an entity's what business risk events are more likely to occur, CEIs would offer objective basis to *confirm* the entity's what business risk events may have happened already, thus help to identify the entity's significant business risks whose controls are not deemed to effective and whose audit implications are greater. We argue that monitoring both leading indicators and CEIs would help auditors better keep track of an entity's business risks and develop their belief about their implications on audit risks and the effectiveness of the relevant risk control activities of the entity.

As described in Figure 10, leading indicators may provide information about antecedents or causes of specific risks, and can therefore be used to estimate risks in the future. CEIs may provide information about the lingering effect of specific risks, thus facilitate to detect the occurrence of the risk events. That is, leading indicators would represent the circumstances or situation before the specific risk occurs, and the CEIs would represent the organization's current business environments after the specific risk has occurred.

For example, consider leading indicators and CEIs for the liquidity risk[24] at a bank. High bid-ask spread, increase in customer loan delinquency, and decrease in earnings (Matz, 2008) are some leading indicators of the liquidity risk. On the other hand, CEIs would

[24] Liquidity risk in general refers to the possibility that the bank cannot meet its obligations for cash demanded from its depositors or through clearing systems (Fields et al., 2004). In CRMA methodology, the liquidity risk would be categorized as process risk (internal risk).

include a downgrade of the bank's rating, which represents the bank's current situation or circumstances after the liquidity problem has occurred.

As such, CEIs provide information that confirms the occurrence of an underlying risk event. Even if leading indicators indicate no signal, CEIs may still show the lingering effects of the previously unanticipated event.

Figure 10 Leading indicators and CEIs

CEIs would help the auditor to identify which risk events have affected relevant business operations and caused related auditable problems. Such materialized risks would also increase the audit risk and the organization's exposure level to that materialized risks.

To provide an example, suppose that the leading indicators for the liquidity risk at a bank show that there is no significant sign of rising liquidity risk, but CEIs show the lingering effects of the organization's past liquidity problems, such as a downgraded rating. This implies that liquidity problems are still affecting the bank, thus the related auditable issues may have happened or more likely to happen, requiring the auditor's attention. For instance, the organization's downgraded credit rating due to their liquidity problems happened in the last year may make them look less appeal to the investors and creditors, despite their improved liquidity management program in this year. In such case, it may be possible that the organization engages in some fraudulent accounting practice to cover up

their poor creditability by choosing not to disclose relevant information or distort the reality.

If only leading indicators are used, the auditor may decide that the organization has a low liquidity risk as their liquidity management programs have been improved, but miss the potential audit risk arising from the lingering effects of past liquidity problems. Both leading indicators and CEIs should be examined to better detect potential auditable issues arising from risk events that are either likely to occur or have occurred already.

Unlike CEIs, leading indicators would provide real-time trend information about a given risk. They together would provide useful information about the current states of the organization's business operations and environment to evaluate which risks are more likely to occur and cause relevant audit concerns to arise in the present or near future.

The proposed CRMA methodology involves the identification of leading indicators and CEIs to be monitored to assess the organization's exposure levels.

3.3.2.2.5 Thresholds: Basis to interpret KRIs

For each leading indicator or CEI, a threshold or limit should be specified in advance (Hwang et al., 2009; Davies et al., 2006, IOR, 2010) and used to determine whether observed values indicate a significant change in exposure level (IOR, 2010). According to IOR (2010), a threshold can be set as a 'cap' or upper boundary, a 'floor' or lower boundary, or a 'collar' combination of cap and floor, within which the indicator values are expected to remain.

To provide an example, consider that a community college monitors number of new students enrolled each academic year as a leading KRI of its operational risk and decides

the threshold for such KRI is a minimum of 500 per academic year. In this case, the threshold level is set at a 'floor' or lower boundary. Without well-defined thresholds, the utilization of KRIs to monitor the exposure level to risks could be inconsistent and confusing (IOR, 2010, Davies et al., 2006).

Determination of threshold level may reflect the organization's risk tolerance and appetite, or management's specific performance targets (Hwang, 2009). The CRMA auditor should consult with senior management or governance to set appropriate threshold levels for each KRI identified. A proper threshold for a particular KRI may be selected by considering the organization's historical averages, management's goals or expectations, or industry benchmarks[25] (Finlay, 2004).

For example, suppose the CRMA auditor is deciding a threshold value for number of delayed or non-delivered purchase orders as a CEI for the organization's requisition process risk. The CRMA auditor may discuss with the auditee's senior management or responsible risk manager to decide the threshold value. Suppose they decided to use the organization's historical average as the threshold for such a CEI for their requisition process risk, and the historical data show that the organization has experienced the requisition order failures 3 times per month on average, then the CRMA auditor would set 4 or 5 as a 'cap' or upper boundary threshold for the KRI. If the CEI value exceeds 4 or 5, this may indicate an abnormal situation and a significant change in the auditee's

[25] Thresholds could be also determined from the external sources, such as the industry standards if given KRIs are commonly used in practice. In fact, some professional organizations such as Risk*Business* and RMA (Risk Management Association) have been initiated to develop a common database of KRIs by industry to be used for benchmarking purpose (Davies et al., 2006; Finlay, 2004). With standardized KRIs, the organizations in the same industry may use them in evaluating their risk exposure levels against their peers and improve their risk management to be more proactive.

requisition process risk exposure level because the value exceeding 4 or 5 is unusual since the average value has been 3. Consequently, the CRMA auditor would plan audit procedures that focus on the requisition ordering process.

3.3.3 Step 3: Measure and monitor selected KRIs for each given business risk

3.3.3.1 Assessment of a risk exposure level by integrating multiple KRIs

To recognize the significant business risks, the proposed CRMA methodology measures the organization's each business risk exposure level. Under the proposed CRMA methodology, the risk exposure level means the extent to which the organization is vulnerable to the given risk and measured by the relevant KRIs. That is, the higher exposure level a risk has, the more vulnerable the organization is to the given risk. It is also assumed that the organization's high risk exposures are considered as the significant risks and subject to the subsequent audit targets[26].

The proposed CRMA methodology assumes that as long as the relevant KRIs are monitored on an ongoing basis, they would provide a real-time information about how vulnerable the organization is against the given risk, facilitating ongoing assessment of the risk exposure level. The proposed CRMA methodology provides an approach to assessing the organization's each business risk exposure level in a continuous and real time manner by using multiple leading indicators and CEIs representing different symptoms and signs of the impact of the organization's each business risk. The proposed CRMA methodology integrates such sub-multiple KRIs for each given business risk into a composite index value to quantify the risk exposure level for each business risk of an organization.

---

[26] We assume that the more vulnerable the organization is to a given risk, the more that given risk is not being controlled. Therefore, the proposed CRMA methodology use the organization's high risk exposures as a basis to determine the subsequent audit plans.

3.3.3.2 Integration of KRIs: creating a composite indicator

To illustrate the multifaceted nature of risk (Scandizzo, 2005), consider software development. If software development risk is not well managed, the organization may suffer from cost overruns, project delays, unmet user needs, and unused systems (Ropponen and Lyytinen, 2000). Boehm and Ross (1989) identified 10 sub-items of software development risk, while Ropponen and Lyytinen (2000) found 6. These researchers suggest that the management of each risk factor would improve the effectiveness of software development projects.

Davies et al. (2006) and IOR (2010) contend that composite or index indicators that combine different KRIs into a weighted value may be more realistic measures of specific risk exposure, rather than KRIs that are individually monitored, such as 'top ten' KRIs to predict what will happen in the future. Such composites are multi-dimensional and could capture broader issues that single KRI alone may not address, such as process quality, technology stability, client satisfaction, etc. (Nardo et al., 2005; Davies et al., 2006).

Integrating different KRIs should capture the multi-dimensional facets of risk factors and provide better information about the risk. In the proposed CRMA methodology, different measures of relevant KRIs are identified and monitored to better capture the multiple facets of the risk and assess its exposure level in the organization more realistically. Individual KRIs are then considered sub-KRIs of the given risk, and each sub-KRI may represent different sources of the given risk or varied symptoms of the presence of the given risk.

The proposed CRMA methodology involves integration of multiple KRIs into a composite KRI index for each risk monitored. This composite KRI index value for each

risk is used as a basis to rank highest risk exposure levels and identify uncontrolled risks in the organization. A higher exposure level to a given risk would mean that the organization is more vulnerable to the given risk.

3.3.3.2.1 Normalization and Aggregation methods

Different measures of KRIs of a given risk may represent different sources of the risk or its varied symptoms, thus they may be measured in different units. KRIs that are measured in different units should be normalized and properly weighted to be aggregated into a composite KRI index representing a particular risk's exposure level (IOR, 2010). Various normalization and aggregation methods have been developed to composite different indicators (Freudenberg, 2003; Nardo et al., 2005). Examples of normalization methods include ranking, standardization, re-scaling, distance to reference, categorical scale, and percentage of annual differences over consecutive years (Nardo et al., 2005). However, assigning proper weights to and aggregating different indicators are more difficult (Saisana and Tarantola, 2002).

There are also a number of weighting and aggregating methods developed for integrating different sub-indicators to compute a composite index for various purposes[27]. Such weighting and aggregation methods range from simple equal weights to statistical

[27] The relevant literature reveals that there are many composite indices that combine different measures of indicators are used to represent the level of performance in certain areas of various fields (Nardo et al., 2005; Saisana and Tarantola, 2002). Some of the examples include Composite Leading Indicators developed by OECD, or Economic Sentiment Indicator measured by the European Commission is used in the Economy field. For Science, Technology and Information, Technology Achievement Index developed by the United Nations (Saisana and Tarantola, 2002). Different indices use different normalization and aggregation methods depending on data property and objectives of the given indices (Nardo et al., 2005; Bandura, 2008). However, researchers point out that selecting proper normalization method is not trivial and requires special attentions as different normalization methods could lead to different results.

analysis-derived weighting methods, such as factor analysis, principal components analysis, data envelopment analysis, analytic hierarchy process (AHP), multiple linear aggression, or geometric aggregations (Nardo et al., 2005).

Rather than using a standardized sub-KRI weighting method, appropriate normalization and weighting methods should depend on the characteristics of the given data (Saisana and Tarantola, 2002; Nardo, 2005). For example, when sub-indicators have the same measurement unit, linear aggregation method is suitable. If the sub-indicators are non-compatible and primarily positive measures expressed in different ratio-scales, geometric aggregation is more appropriate (Nardo, 2005). Therefore, we do not prescribe specific normalization and weighting methods for the proposed CRMA methodology. However, when it is implemented, the CA auditor should brainstorm and select appropriate methods for normalization and weighted aggregation based on the characteristics of given sub-KRIs.

3.3.3.3 Examples for KRI integrations

3.3.3.3.1 Normalization

Consider the following as an example of sub-KRI normalization and weighting. Here, normalization is achieved by measuring the ratio of the observed value of a given KRI to its threshold (benchmark) in general[28][29].

$$Normalized\ KRI = \frac{Value}{Threshold\ (max)}$$

[28] Similar method (named as distance to reference) is referred as a normalization method to normalize the indicators to develop a composite indicator to represent the country performance, along with other methods (Nardo et al., 2005)

[29] Scandizzo (2005) used similar equation: a normalized KRI = $\frac{a}{\max(a)}$ where max(a) is the maximum value indicator a can take. However, he did not address the potential shortfall of such method when finding a maximum value is not ideal, but minimum or between maximum and minimum is more reasonable.

However, this ratio based normalization method should be modified for the different types of threshold setting, such as ‘cap’, ‘floor’, or ‘collar’ (IOR, 2010, p.11) used for each different sub-KRI in order to obtain a comparable normalized KRI value expressed in the same unit scale so that different sub-KRIs can be integrated meaningfully. For instance; if a threshold of a given KRI is set at an upper boundary (maximum value), actual values that exceed this threshold level may indicate a change of exposure. If the threshold is a lower boundary (minimum), actual KRI values that are greater than the minimum are normal, but when those below the minimum represent an unfavorable change in exposure level. If a threshold is set between minimum and maximum boundaries, all values between the two threshold points are viewed as normal, but values out of the range in either direction may represent rising risk exposure.

Therefore, we present following ratio based normalization equations modified for different setting of thresholds:

If the threshold is set as a maximum:

$$Normalized\ KRI = \frac{Value}{Threshold(max)}$$

If the threshold is set as a minimum:

$$Normalized\ KRI = \frac{Threshold(min)}{Value}$$

If the threshold is set with both minimum and maximum points:

$$Normalized\ KRI = \frac{\frac{Value}{Threshold\ (Max)} + \frac{Threshold\ (min)}{Value}}{2}$$

Using such normalization techniques reflecting different types of threshold settings, we assume that multiple sub-KRIs with different threshold types would be transformed into the same scale and unit to be aggregated properly. In this normalization method, the higher (lower) a normalized KRI value, the more (less) significant change in the risk exposure level it may represent, since the normalized KRI value would become greater as its actual value continues to exceed the threshold.

3.3.3.3.2 Weighting and Aggregation

Along with normalization, weighting each sub-KRIs is a required step to aggregate multiple sub-KRIs into a composite index value (Saisana and Tarantola, 2002; Nardo, 2005). As an example, let us use the equal weight method (Saisana and Tarantola, 2002).

Using this method, different KRIs can be converted into the same unit scale and aggregated to produce a composite index. In equation, the aggregation methods used in this example can be expressed as

$$\textit{KRI Index (Risk Exposure level)} = \frac{\sum_{i=1}^{n} normalized\ KRI\ (i) * weight\ (i)}{\sum_{i=1}^{n} weight\ (i)}$$

To provide an example how this normalization and weighting methods aggregate different multiple sub-KRIs of a given into a composite KRI index value, suppose that a CRMA auditor at a financial institution monitors its liquidity risk levels with four KRIs: ‘decline in earnings’, ‘decline in stock price’, ‘significant asset acquisitions’, and ‘downgrading by a nationally recognized rating organization’ (Matz, 2008), and uses the normalization and weighting method described above to integrate them into a KRI index value. We generated KRI values and thresholds for this example. Using the

aforementioned normalization and weighted aggregation methods, a KRIs based index value is computed as shown in the Table 3.

Liquidity Risk (Sub-KRIs)	*Threshold*	*Value*	*Weight (Equal Weight Method)*	*Normalized value (Value/Threshold)*	*Total (Weight*Normalized score)*
KRI 1: Decrease in earnings (Leading)	-5% (max)	-3%	1	0.6	0.6
KRI 2: Decrease in Stock price (Leading)	-5% (max)	2%	1	-0.4	-0.4
KRI 3: Increase in Asset acquisition (Leading)	+10% (max)	2%	1	0.2	0.2
KRI 4: Decreased in credit rating (CEI) i.e., coding scheme: AAA:6;AA:5;A:4 BBB:3,BB:2,B:1	BBB (min)	A	1	0.75	1
Liquidity risk exposure level ($\frac{\sum_{i=1}^{n} normalized\ KRI\ (i) * weight\ (i)}{\sum_{i=1}^{n} weight\ (i)}$)					0.35

Table 3 Liquidity risk exposure level

With appropriate normalization and weighted aggregation method, multiple sub-KRIs that represent the multi-dimensional symptoms and sources of a given risk would be aggregated properly into a composite index value that better indicates the exposure level of a given risk[30].

The proposed CRMA methodology uses such an integrated KRI based index value in prioritizing the organization's risks and the subsequent audit procedures. As discussed earlier, under the proposed CRMA methodology, it is assumed that a higher index value of a given risk may mean that the organization's exposure level to the given risk is greater.

[30] Depending on which normalization and weighting methods are used to aggregate sub-KRIs, the resulting index value may be different (Nardo, 2005), thus the CRMA auditor should be able to select appropriate normalization and aggregation methods to achieve quality results.

3.3.3.3.3 Ranking risk exposures

Since greater risk exposure may have audit implications (Lemon et al., 2000; Bell et al., 1997; Eilifsen et al., 2001; Knechel, 2007), the subsequent audit procedures should be relevant to those high level risk exposures. Therefore, the proposed CRMA methodology requires ranking the organization's risk by exposure level, measured from their relevant KRIs, and determining the priority of the relevant audit and risk management procedures to mitigate their adverse impacts on both RMM and management's business and risk management processes.

To provide an example of how the proposed CRMA methodology ranks the organization's risks, suppose that the CRMA auditor at the financial institution in the previous example also monitors operational risk with four KRIs: total number of robberies, total number of card transactions disputed by customers and clients, total number of cards issued, but reported stolen, and total number of customer e-banking accounts compromised due to phishing attack or Trojans (IOR, 2010). Using the same methods for normalization and weighting used in the previous example and hypothesized KRI values for those four KRIs, a composite KRI based index value representing the operational risk exposure level is shown in Table 4.

Operational Risk (Sub-KRIs)	*Threshold*	*Value*	*Weight (Equal Weight Method)*	*Normalized value (Value/Threshold)*	*Total (Weight*Normalized value)*
KRI 1: Total number of robberies (monthly basis; CEI)	3 (max)	0	1	0	0
KRI 2: Total number of credit card transaction disputes (monthly basis; Leading)	20 (max)	38	1	1.9	1.3
KRI 3: Total number of credit cards reported stolen (monthly basis; Leading)	25 (max)	30	1	1.2	1.2
KRI 4: Total number of phishing or other cyber-attacks (monthly basis ; Leading)	10 (max)	20	1	2	2
Operational risk exposure level ($\frac{\sum_{i=1}^{n} normalized\ KRI\ (i) * weight\ (i)}{\sum_{i=1}^{n} weight\ (i)}$)					1.125

Table 4 Operational risk exposure level

For these particular hypothesized data, the operational risk exposure level is computed as 1.125. Compared to the liquidity risk exposure level computed in the previous example shown in Table 3, this index value is greater than the liquidity risk exposure level, 0.35. Therefore, under the proposed CRMA methodology, operational risk is considered more significant than liquidity risk, meaning that the organization is more likely to be affected by inefficient business operations than by liquidity problems (Table 5).

Risks being monitored	Index value	Ranking
Operational risk	1.125	1
Liquidity risk	0.35	2

Table 5 Risk Ranking for recognizing highest exposure risks

So far we have discussed that the proposed CRMA methodology encompasses the identification of the organization's risks to be monitored, selection of relevant KRIs, and

normalizing and aggregating them for each selected risk monitored to derive a composite index to measure each risk's exposure levels in the organization. In the next section, we discuss prioritizing audit and risk management procedures which is the last step of the proposed CRMA methodology.

3.3.4 Step 4: Prioritization of Audit and Risk Management Procedures

Once each risk is ranked by index value, the next step is to prioritize audit and risk management procedures corresponding to the organization's highest risk exposures. In the proposed CRMA methodology, the objective of the prioritization of audit and risk management procedures is to minimize audit risk and the organization's risk exposure. If the relevant audit and risk management procedures that address the organization's current highest risk exposures are prioritized, risk exposure, and thereby RMM and audit risk, would be reduced.

In the previous example, the organization's operational risk exposure was higher than its liquidity risk. In this case, under the proposed CRMA method, the audit and risk management procedures that focus on the organization's high operational risk exposure would be prioritized over those related to the liquidity risk. In the following section, we discuss how the proposed CRMA methodology links the organization's business risks assessments to the prioritization of the relevant audit and risk management procedures.

3.3.4.1 Prioritization of audit procedures

3.3.4.1.1 Linking uncontrolled risks to corresponding audit procedures

In order to prioritize audit procedures based on the organization's risk exposure levels, there must be a linkage between the organization's risks and the corresponding audit procedures. However, as discussed earlier, the extant literature lacks in guidance on how auditors can link their understanding of the client's business strategies, processes,

environment, and related risks to the affected audit risks and subsequent audit procedures (Robson et al., 2007; Knechel, 2007, PCAOB, 2005). Since the organization's business risks are often related to non-accounting information, it is challenging for the auditor (used to dealing with accounting information) to link the organization's business risk information to appropriate subsequent audit procedures required to reduce audit risk (Knechel, 2007). Some researchers attribute the difficulty of implementing a risk based audit to the subtle relationship between the organization's business risks and the appropriate audit responses (Knechel, 2007; PCAOB, 2005). The proposed CRMA methodology fills this gap by offering an approach to linking the organization's risks to corresponding audit responses.

3.3.4.1.2 Ongoing prioritization using pre-established links

The proposed CRMA methodology provides an ongoing linking process between the organization's business risks to corresponding audit procedures so that the previously planned audit procedures can be quickly adjusted whenever new significant risks arise. To end that, the proposed methodology utilizes pre-established links that map the organization's selected business risks to be monitored to their pre-configured corresponding audit procedures. Such pre-established links would work as a mapping tool that allows for immediate selection of audit procedures in response to changes in the organization's risk exposure levels.

To build a pre-established link, the CRMA auditor would need to go through at least two steps as shown in Figure 11; first the CRMA auditor maps each monitored risk to potential auditable issues or problems. The second step is to configure appropriate audit procedures to address the identified auditable issues or problems for each risk.

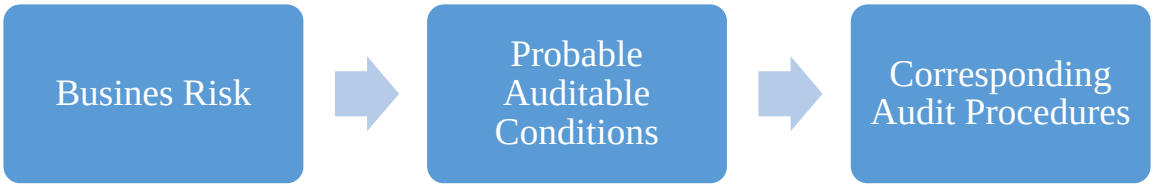

Figure 11 Process of linking business risk to its corresponding audit procedures

Corresponding audit procedures for the organization's given risks are determined by the probable auditable issues that could be brought by that given risk. Such issues are concerns or conditions that could result in increased audit risks for the given audit subject matter. For example, auditable issues for the financial statement audit would be any potential condition or concern that could result in undetected material financial misstatements, thus increasing the risk that the auditor may provide a wrong opinion on the fairness of the organization's financial statements. Likewise, for IT audit, the auditable issues would be any problem or condition that may lead to ineffective IT systems, such as vulnerable IT structure or unknown weak controls that may potentially hurt the soundness of IT systems, increasing the risk that the auditor may not detect such ineffectiveness in the organization's IT systems. For a fraud audit, the auditable issues would be situations or issues that may create opportunities for management or employees to perpetrate fraud and remain undetected. For a risk management audit, the auditable issues would include any condition or event that may signal weak risk controls and ineffective risk response strategies that are not known before the audit. Knowing such possible auditable issues and issues would help the auditor to develop specific, corresponding audit and risk management procedures for each major business risk the organization faces.

Suppose that change in the price of raw material is a major risk for a manufacturer[31]. If the raw material purchase price risk is materialized, meaning that the raw material purchase prices have gone up unacceptably high, the company's production costs would increase and its profitability would go down. The company may manage such a risk by entering future contracts on the prices of raw materials or successfully passing on increased production costs to customers. If these risk management strategies are working effectively, the company may ensure its profitable business operations, but if not, the organization' s profit margins would decrease (Knechel, 2007).

Such circumstances may increase the management's motivation to distort the related financial and business performance records to hide the adverse impacts of such a risk on their business operation. A low material price with a rising trend still indicates a likelihood of such an adverse situations is higher, thus audit risk increases as well. Thus, when the company's raw material purchase price risk exposure level is high, the auditor would need to plan substantive audit procedures that address whether the organization's business transactions relevant to the raw materials are properly recorded and relevant accounts and assertions are correctly values and reported.

Potential auditable issues which could be raised by a particular risk can be identified in advance by assuming that the given risk has already materialized. With the potential auditable issues from each risk being monitored in the organization, corresponding audit procedures can be configured in advance, creating linkages between organizational and audit risk.

---

[31] This example is adopted from Knechel (2007) and used elsewhere in Ch2 of the present paper.

The proposed CRMA methodology uses links that connect organizational risk to auditable issues, and then to pre-configured audit procedures. Using such pre-established links, the proposed CRMA methodology allows for the immediate selection of appropriate audit procedures in response to changes in the organization's high risk exposures. This mechanism offers dynamic audit procedure planning that adjusts current audit plans in response to changes in the organization's monitored risk exposure levels.

3.3.4.2 Prioritization of risk management procedures

CRMA also prioritizes organizational risk management procedures to mitigate potential business and risk management adversity. As appropriate risk management procedures corresponding to the organization's highest risk exposures are prioritized and performed first, the likelihood of the adverse effects of those high exposure risks would be reduced, thus the organization's risk exposure levels and the affected audit risk would be also minimized.

Likewise, the rationales for prioritizing risk management procedures for the organization's manager are twofold in the proposed CRMA methodology. First, the prioritized risk management procedures that address the organization's ineffective risk management control activities would be value-added feedback for the organization's manager to lower risk exposure levels and improve risk management process effectiveness.

Second, knowing ineffective risk controls and risk management processes would enable the auditor to perform value-added risk management assurance services in addition to fulfilling the given audit task. Today's internal auditors are increasingly asked to provide objective evaluation of the organization's risk management processes and assist

management to maintain and improve quality risk management initiatives (PwC, 2015a; Gramling et al., 2003). Given that the organization's business risks change constantly, the ability to recognize changes and identify newly emerging risks would be critical for ensuring successful business operations. The ability to obtain timely information about ineffective risk management controls and the priority of risk management procedures addressing them would help the internal auditor to meet such new demand. With this rationale, the proposed CRMA methodology entails the prioritization of risk management procedures.

For external audit to provide an opinion on the organization's financial statements, an understanding of risk management procedure priority would not be necessary beyond knowing the effects of such high level risks on the audit risk of the given financial statement audit in a continuous manner (SAS No. 109, AICPA, 2006b). The proposed CRMA method may help the external auditor to quickly recognize changes in the organization's business risks and ineffective risk management controls activities and link them to relevant audit procedures.

For internal audit functions, the evaluation of the effectiveness of the organization's risk management process, internal controls, and corporate governance is explicitly stated as one of their responsibilities (IIA, 2012). Prioritizing the risk management procedures in light of the organization's current high level risks would facilitate the internal auditor to fulfill their role in evaluation on the effectiveness of the organization's risk management process.

3.3.4.2.1 Ongoing prioritization of risk management procedure using pre-established links

The proposed CRMA methodology also utilizes pre-established links between the organization's business risks and their corresponding risk management procedures that examine their risk management control activities and policies.

Establishing the links between the organization's business risks and their corresponding risk management procedures would be more straightforward than mapping to their corresponding audit procedures. That is, the organization's each risk is mapped to its control activities designed to mitigate its adverse effects, and to relevant risk management procedures that evaluate the effectiveness of such control activities. With such pre-established links, risk management procedures to check the effectiveness of control activities are related to current high risk exposures would be automatically selected as they emerge. Such ongoing prioritized risk management procedures would enable the auditor to provide timely assurance on the organization's risk management process, which is increasingly emphasized as a new role for internal audit functions.

Figure 12 Process of linking business risks to corresponding risk management procedures

To illustrate how the pre-established links are used for ongoing prioritization of audit and risk management procedures, consider the examples provided earlier with the financial

institution that monitors its liquidity and operational risk exposure levels. Assume that the CRMA auditor monitors only these risks for their financial and internal control audit. Under the proposed CRMA methodology, these two risks would be monitored and assessed through their relevant KRIs and their risk exposure levels would be ranked to evaluate which risk is more significant. The pre-established link would automatically identify corresponding audit and risk management procedures to the highest level risks.

As for an example, suppose that the pre-established links for the audit procedures for the auditor and risk management procedure for the organization manager are made as in Table 6 and 7 respectively.

Risks being monitored	Auditable issues (financial statement and internal control audit)	Audit Procedures
Operational risk (internal)	• Unauthorized activity • Theft and Fraud • Vulnerable Systems Security • Unsafe Work Environment	• Test the internal controls related to segregation of duties and safe guarding assets • Perform detail test on transactions related to the inefficient process • Examine the adequacy of operational risk capital
Liquidity risk	• Non-compliant off-balance sheet activities • Failure to meet liquidity risk disclosure requirements • Going concern and insolvency problems	• Investigate the adequacy of fair-value measurements and off-balance sheet transactions • Examine the adequacy of liquidity risk disclosure • Examine fairness of loan impairments • Examine the capability to repay debts from operating cash flows

Table 6 Pre-established link for Audit Procedures

Risks being monitored	Risk Controls	Risk Management Procedures
Operational risk	• Safety Training • Data capture • IT systems • Turnover	• Examine whether the safety training programs are running as intended • Ensure operational loss data is collected • Examine HR programs to retain key employees • Examine the effectiveness of IT systems
Liquidity risk	• Contingency funding plans • Funding limits • Liquidity risk management rules and policies	• Examine appropriateness of contingency plan • Assure the effectiveness of liquidity risk management rules • Assure the compliance with the established funding limits

Table 7 Pre-established link for Risk Management Procedures

Suppose the organization's operational risk exposure level is higher than their liquidity risk exposure level, then the pre-configured audit and risk management procedures designed for the operation risk would be prioritized as the subsequent audit plan and risk management activity that the auditor and management, respectively, should focus on. However, if the conditions changed and the liquidity risk exposure level turns to be higher than the operational risk, then the audit and risk management procedures previously configured for liquidity risk would be prioritized over those for operational risk.

Summary of the proposed CRMA methodology

Steps	***Summarized Key Procedures and Purposes***
Step 1: Identify the organization's risks to be monitored.	▪ To ensure all significant potential adverse events (risk events) are considered, a three class scheme is used: Process (internal) risk, Environmental (external) risk, and Black Swan (rare and unknown). ▪ Select the most critical and significant risks to the organization.
Step 2: Select relevant KRIs (leading indicators and CEIs) of the selected risks to be monitored.	▪ KRI is any type of data or metric that provides information about the current status of a given risk, whether it is rising (leading) or the effects of a given risk occurred already (lagging). ▪ Relevant KRIs are selected to monitor a given risk as there could be multiple symptoms of the presence of given risk. Each KRI (leading indicator or CEI) may represent different sources of the given risk or unique phenomena or situations associated with the presence of the given risk.
Step 3: Measure and monitor selected KRIs of each given risk and its exposure level in a continuous manner, so that significant change in the organization's risk profiles can be	▪ To better catch multi-dimensional risk symptoms and sources, different measures of KRIs for each risk are combined into a weighted index value, which is used as an indicator of the given risk's exposure level.

detected in a real time manner.	▪ Given appropriate normalization and aggregation methods, different measures of KRIs are transformed into the same unit scale and integrated to produce an index value that indicates its exposure level in the organization. ▪ Continuously monitor relevant KRIs of each given risk and its exposure level.
Step 4: Prioritize audit and risk management procedures in an ongoing manner so that the priorities of audit and risk management procedures can be adjusted whenever changes in the organization's risk profiles occur.	▪ The objective of prioritization is to minimize the organization's risk exposure level and affected audit risk. ▪ Rank all risks that are being monitored by index value. ▪ Match each risk ranked to its pre-configured audit and risk management procedures in an ongoing manner, thereby all audit and risk management procedures are prioritized in a real time manner.

Table 8 Key steps and procedures in the proposed CRMA methodology

3.4 Conclusion and Remarks

In this chapter, we propose a methodology for CRMA drawing on the original suggestions in Vasarhelyi et al. (2010). The motivation of CRMA is to shift a static CA system to a risk driven dynamic system which responds to the organization's constantly changing risk environments and adjusts existing audit procedures as needed. Vasarhelyi et al. (2010) describe CRMA as a new procedural component of a CA system that

complements other CA procedures, CDA or CCM (Figure 7). CRMA makes CA more effective and robust against the organization's constantly changing risk environments.

As summarized in Table 8, the proposed CRMA methodology consists of four steps and utilizes relevant KRIs in monitoring and assessing the organization's risk exposure levels in real-time. As relevant KRIs are measured in a real time manner, they would provide real-time information to indicate the current development of a given risk, such as whether the risk is rising, remote, or materialized already.

In the proposed CRMA methodology, multiple relevant KRIs are identified and combined into a composite index value which is then used to quantify a given risk's exposure level. As each relevant KRI may represent multi-dimensional sources and/or symptoms of the given risk, a composite index value would better catch changes in the given risk's exposure level.

To enable ongoing prioritization of audit and risk management procedures in response to changes in the organization's significant risk profile and affected audit risks, the proposed methodology uses pre-established links that connect each monitored organizational risk to potential auditable issues (risk control activities) and pre-configured audit procedures (risk management procedures) that address the identified potential auditable issues. By matching the highest risk exposure levels (indicated by their highest index values) to their pre-configured audit or risk management procedures, the subsequent audit and risk management procedures are prioritized in a consistent and automated manner.

The priority of the risk management procedures arranged by the organization's highest risk exposure levels would be valuable feedback for the organization to improve risk management processes or useful input for the internal auditor to plan their internal audit activity to evaluate the effectiveness of the organization's risk management process. In the CA context, the prioritized risk and audit procedures from CRMA can be useful input to other ongoing CA procedures, such as CCM or CDA to direct them to the areas of high risks.

3.4.1 Focusing on real time data

The proposed CRMA methodology is a data-centric method that utilizes KRIs to assess the organization's current risk exposure levels in a timely manner, rather than estimating the likelihood of the organization's particular risk events by relying on probabilistic risk models which use historical frequency data (Stulz, 2008, 2009). A KRI is data or a metric that provides information about the current state of a given risk (IOR, 2010). The quality of KRIs and ability to collect them in a real time manner would determine the effectiveness of the proposed CRMA methodology.

From this perspective, among other required steps of the proposed CRMA methodology, identifying and obtaining best available relevant data of KRIs in a real time manner would be the most critical to implementation. If relevant KRIs representing the current status about a given risk are not measured and monitored in real time, the assessments of the organization's current risk exposure levels would be hindered. Therefore, the ability to identify and measure relevant KRIs in a real time manner would be the most important initial requirement of the proposed CRMA methodology.

As a CA procedure, CRMA takes advantage of ongoing data analytics and monitoring programs in the given CA system such as the monitoring and control (MC) layer (Vasarhelyi and Halper, 1999; Vasarhelyi et al., 2004) that are connected to the organization's automated and integrated IT systems, as well as external information sources as needed, to extract real-time business process data, performance metrics, or other third-party provided information to measure and monitor relevant KRIs of the organization's risks. Use of such continuous data monitoring and analytics would make it more efficient to collect and monitor relevant KRIs in real time.

3.4.2 Big Data and KRIs

In the Big Data[32] era, companies strive to use all available data they can collect to improve their business (Dean, 2014). Today's environment is flooded with enormous volumes of data from wide range of data sources in many forms: structured or unstructured, text or images, internal or external, etc. (Dai et al., 2012). A recent PwC Global Survey (PwC, 2015b) reports that the majority of CEOs believe that digital technology and data analytics skills add value and improve the organization's competitiveness and capabilities.

With proper data management systems and mining tools, the organization measures and monitors business operation statuses and performance results in real time (Manyika et al., 2011). Such real-time operational data and performance metrics would enrich data resources for the organization to develop relevant KRIs to monitor and measure the organization's risks. Utilizing all available data and information, the CRMA auditor

[32] Big data means that the size of data could be well beyond a given organization's ability to handle with their standard database systems and software (Manyika et al., 2011).

would better identify or develop quality KRIs that represent the organization's risk exposure levels.

3.4.3 Limitations and Future research

According to the original framework (Vasarhelyi et al., 2010), CRMA takes advantage of the organization's automated and integrated IT systems and computerized algorithms to continuously monitor and assess the organization's risks levels and automatically prioritize the subsequent audit procedures to minimize the audit risk and the organization's risk exposure levels on an ongoing manner. The present study reviews this original work on CRMA, its underlying motivations, and its purposes. We propose a methodology for CRMA to assess and monitor the organization's risk exposure levels, how the changes in the organization's risks can be recognized in a real time manner, and how the relevant audit and risk management procedures can be prioritized and re-prioritized automatically whenever changes in the organization's risk profiles occur. The design of specific algorithms and prescriptive normalization and weighting methods for these procedures is are beyond the current study and we leave it for the future research agenda.

CRMA is initially proposed as a third procedural component of CA system, which interacts with other CA procedures, CDA or CCM. If CDA and/or CCM procedures are continuously adjusted by input from CRMA, they would become risk based CA procedures that focus on high risk areas, thereby shifting the underlying CA system into a risk responsive dynamic system. Therefore, linking CRMA to CDA or/and CCM would be critical to changing a static CA system to a risk driven system. However, the present

study lacks guidance on that matter as we limit our focus on CRMA. We leave this important research agenda for the future study.

Given that the organization's risks are constantly changing, timely recognition of changes in the organization's risk profiles would be critical to an effective risk based audit. Delayed or untimely recognition of newly arising uncontrolled risks in the organization may cause the auditor to fail to detect consequential effects on the audit risk, hindering the effectiveness of the subsequent risk based audit plans. From this perspective, continuous risk assessments that recognize changes in the organization's risk exposure levels and adjusts existing audit plans in an ongoing manner would be necessary for an effective risk based audit.

Chapter 4: Monitoring an organization's reputation risk exposure level with KRIs: Using Twitter data to detect a sign of the reputation damage in real time

4.1 Introduction

The auditor's ability to quickly assess and recognize changes in the organization's risk profile and their impacts on the audit risks is vital to the risk based audit (Bell et al., 1997). In this chapter, we demonstrate how the proposed CRMA methodology could be used for such purpose by discussing monitoring and assessment of the company's reputation risk in a near-real time manner. In doing so, we present a KRI (Key Risk Indicator, IOR, 2010) that represents the degree of the public's negative perception of the company. The present KRI is measured from comments posted on social media, a source of real time information about changes in public perception. We measure the present KRI using Twitter data surrounding two historical events: Purina's lawsuit for selling harmful dog food (CNN, 2015) and Starbucks' "Race Together" campaign (WSJ, 2015).

Real-time monitoring and assessment of KRIs is critical to the proposed CRMA methodology. Quality KRIs may originate from both internal and external sources (Beasley et al., 2010). For example, internal KRIs may include business operational performance metrics or relevant financial records, such as number of unresolved customer complaints, staff turnover ratio, average amount of losses, defective production rate, etc. External KRIs may include unemployment rate, third party customer surveys, exchange rates, bond ratings, or stock market index.

Big data may provide unprecedented resources for organizations enhance self-knowledge and improve their strategic decision making process (McAfee et al., 2013). Many large

companies have already invested in big data collection and analysis (Manyika et al., 2011; Davenport and Dyché, 2013).

The proposed CRMA methodology promotes using all available data sources to discover quality KRIs to more accurately and timely measure the organization's risk exposure levels. The auditor may find useful information to develop quality KRIs by analyzing the organization's internal business process data or relevant external data. Since a KRI is a piece of data indicating the status of a given risk, as long as it is provided in a real time manner, the given risk's exposure level would also be monitored in real time. The proposed CRMA methodology requires the auditor to consider all available internal and external data sources to find useful sources for KRIs. The CRMA auditor would need to not only understand the traditional data sources such as performance metrics, accounting records, transactional business process data, etc., but also analyze the organization's big data sources obtained from their highly automated internal business processes or accessible external sources such as news, social media, etc. in order to obtain quality KRIs to monitor risk exposure.

Comments posted on social media websites and forums such as Facebook, Myspace, LinkedIn, Reddit, Twitter, etc. can be a rich source of external KRI data. These databases are easy to use, are updated in real time, and can quickly change public opinion, trends, and agendas on topics that range from products and services, to the environment and politics, to technology and entertainment (Pang and Lee, 2002; Asur and Huberman, 2008). Such data from the real time social media websites may be used as a KRI to keep track of the public's perception of a particular company, their products or services, or

their corporate image in a more immediate manner. A shift in perception may signal a high risk of damage to the company's reputation.

In this chapter, we provide an example to measure the reputation risk exposure level by utilizing KRIs from the risk based auditor perspective. In doing so, we present such a KRI that measures the degree of negative sentiments expressed in comments posted on social media or Internet forums. More specifically, it measures the proportion of negative polarity to the all positive and negative polarity embedded in social media data. Such KRI would be useful as a CEI to monitor and assess the current effect of the company's risk events on their corporate reputation.

People use social media channels or web based applications to post their opinions on various topics in real time (Pang and Lee, 2008). The proposed KRIs measured from such social media data may allow the auditor to understand how people perceive the organization in a close to the event manner, helping to better assess the organization's current reputation risk exposure. Increasing negative perception may indicate reputational damage.

To demonstrate the present KRI, we use recent reputational risk events involving Purina (CNN, 2015) and Starbucks (WSJ, 2015) and the tweets (Twitter messages) mentioning them. We measure the present KRI from the public's Twitter response to these two risk events, which represent the degree of the public's negative perception of these events. For each reputational event, we downloaded relevant Twitter messages through Twitter's API.

Twitter is a multi-language, worldwide social networking and micro-blogging website available in more than 30 different languages. According to Statista[33], the number of monthly active Twitter users (i.e., unique user) has exceeded 300 million worldwide as of 2015, making it the 8th most popular social networking website worldwide. Among those, 48.4 million active users are from the US (22%) as of 2014 and the number is expected to grow to 53.1 million in 2015.

In the remainder of this chapter, we provide a literature review on corporate reputation focusing on definitions and current measurement practices, and then we discuss how relevant KRIs are used to assess and monitor the organization's reputation risk exposure level under the CRMA methodology concept. Finally, we demonstrate the proposed KRI using two real reputational events and the Twitter response to these events.

4.2 Corporate Reputation

Corporate reputation has been a growing research area in diverse fields including economics, marketing, management, psychology and sociology (Barnett et al., 2006; Ponzi et al., 2011). Many articles in the field have been published since the inaugural issue of Corporate Reputation Review by Fombrun and van Riel (1997) (Barnett et al., 2006)[34]. While the subject of corporate reputation has gained increasing popularity in various academic domains, there is no common definition or operational measure of the corporate reputation of a company, thus its concept and operationalization remain unclear (Chun, 2005; Barnett et al., 2006).

---

[33] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[34] The average number of scholarly publications focusing on corporate reputation between 2001 and 2003 was five times than the one of those published between 1990 and 2000 (Barnett et al., 2006).

As shown in Table 9, Fombrun and van Riel (1997) initially identified six distinct research perspectives on corporate reputation: economic, strategic, marketing, organizational, sociological, and accounting. Numerous theoretical bases are used to support these different conceptions of corporate reputation such as the resource-based perspective, transaction cost economics, signaling theory, and social status (Bergh et al., 2010).

Different views of Corporate reputation	Implications of Corporate reputation
Economist	• Traits or signals to external parties • "Perceptions of firms held by external observers" • Management can make use of corporate reputation to signal the attractiveness strategically
Strategic	• Assets and mobility barriers (barrier to move from one strategic group to another) • Reputations are difficult to duplicate because they derive from unique internal features of firms. • Reputations are externally perceived, and so are difficult to control by firms' managers (Fombrun and Shanley, 1990)
Marketing	• In marketing research, 'reputation' is often labeled as brand image that result in 'pictures in the heads' of external subjects (consumers) about products or services
Organizational	• Reputation is viewed as what shapes the organization's culture and identity shared by employees.
Sociological	• Reputations are considered as indicators of legitimacy in an institutional field. • Reputations are aggregate assessments of firms' performance relative to expectation and norms in the society.
Accounting	• Reputation is viewed as an intangible asset that generates value • Reputation building activities such as R&D activities, advertising, and training expense should be measured and capitalized properly.

Table 9 various views of corporate reputation by different literature (Fombrun and Van Riel, 1997).

Reflecting these characteristics of the construct of corporate reputation, Fombrun (1996) defines corporate reputation as:

"a perceptual representation of a company's past actions and future prospects that describe the firm's overall appeal to all its key constituents (stakeholders) when compared to other leading rivals" (Fombrun, 1996, P72).

Since then, many researchers have provided their definition of corporate reputation (Barnett et al., 2006). Barnett et al. (2006) conducted a lexicological analysis of 49 definitional statements of corporate reputation and identified three clusters of meaning in them based on their similarities: awareness, the most common meaning which emphasizes that reputation is a general awareness or perception[35] of a firm held by observers or stakeholders, but no cognitive judgement about the company's reputation; assessment, which indicates that corporate reputation is opinions or beliefs based on observer judgment, estimation, evaluation, or gauging; and an asset perspective, presuming that corporate reputation has quantifiable economic value.

Barnett et al. (2006) also distinguishes corporate reputation from 'corporate identity' which is underlying character or behavioral symbols of the corporation held by internal people, making it distinctive from others, from 'corporate image'[36] which is observers' (external and internal) general impressions of the corporation's distinct character (i.e.,

[35] Researchers also use other terms such as aggregation of perceptions, latent perceptions, net perceptions, global perceptions, perceptual representation, or representations of knowledge or emotions in stating their definition of corporate reputation (Barnett et a., 2006)

[36] Gary and Balmer (1998) define image is "what comes to mind when one hears the name or sees the logo" of a particular firm (cited in Barnett et al., 2006).

corporate identity), and from ‘corporate reputation capital’ which refers to economic and intangible asset quality of corporate reputation. They assert that corporate reputation is the stakeholders’ collective judgments about the firm’s identity and impressions of its image and often formed as a result of a firm’s visible actions or mistakes, such as ‘environmental damage’ or ‘human rights violations’ events. They define corporate reputation as following:

“Corporate reputation is observers’ collective judgments of a corporation based on assessments of the financial, social, and environmental impacts attributed to the corporation over time” (Barnett et al., 2006).

Although there are various theories and perspectives on corporate reputation in different contexts, it is commonly accepted that corporate reputation is a valuable asset that provides sustainable competitive advantages which are rare, valuable and difficult for a competitor imitate (Ponzi et al., 2011; Schwaiger, 2004; Roberts and Dowling, 2002; Flanagan and O’Shaughnessy, 2005). Researchers found that firms with strong reputation sustain superior financial performance (Roberts and Dowling, 2002), enjoy a lower cost of equity capital (Cao et al., 2015), produce high quality financial reports (Cao et al., 2012), and attract more loyal customers and quality employees (Eccles et al., 2007). Consumers may pay a premium for the products and services of firms with high reputation since reputation is a signal of underlying quality (Sharpiro, 1983). Potential customers receive advertising claims of firms with high reputation more favorably, facilitating marketing initiatives (Goldberg and Hartwick, 1990).

4.2.1 Measuring Corporate Reputation

Since corporate reputation is intangible as a set of belief or perceptions about the company’s past and future actions among its stakeholders, it is difficult to measure (Ponzi

et al., 2011). However, there is a variety of measurement tools developed to measure corporate reputation (Fombrun et al., 2000, Schwaiger, 2004). The most popular corporate reputation measure is Fortune's America's Most Admired Companies (AMAC), released every year since 1982 (Ponzi et al., 2011). AMAC measures corporate reputation based on ratings of companies on eight attributes assessed by industry experts such as senior executives, outside directors, and analysts. The attributes include innovativeness, quality of management, long-term investment value, community and environmental responsibility, ability to attract, develop, and keep talented people, quality of product or services, financial soundness, and use of corporate assets (Schwaiger, 2004). Similarly, Rayner (2004) asserts that corporate reputation is driven by seven attributes: financial performance and long-term investment value, corporate governance and leadership, corporate social responsibility, workplace talent and culture, delivering customer promise, regulatory compliance, and communications and crisis management.

However, researchers find that AMAC's corporate reputation scores are highly influenced by the previous financial performance of companies, discounting other factors of corporate reputation, suggesting a financial halo (Fryxell and Wang, 1994; Brown and Perry, 1994). Dowling (2006) assumes that this effect is attributable to AMAC's use of industry insiders in rating the companies, excluding other stakeholders' perceptions (Fryxell and Wang, 1994; Schwaiger, 2004; Ponzi et al., 2011).

Besides Fortune's corporate reputation measures, there are various corporate reputation scales distributed by consultants or business media outlets around the world. Fombrun (2007) identified 183 public lists that rate or rank companies in over 38 countries. He found that the majority of the lists were based on either a measure of overall reputation

(61 out of 183) or of the workplace, i.e., good company to work for (73 out of 183). The remaining public lists use corporate citizenship, performance, innovation, governance, or products in rating or ranking companies.

Some academic researchers have proposed alternative corporate reputation measures. For example, Fombrun and a market research firm, Harris Interactive, developed a corporate reputation measure referred as the Reputation Quotient (RQ)[37] in 2000. RQ rating is calculated using a 20-item instrument which can be categorized into six attributes: emotional appeal, financial performance, products and services, social performance, vision and leadership, and workplace environment (Ponzi et al., 2011; Fombrun et al., 2000). Fombrun et al. (2000) assert that RQ reflects multiple stakeholders' perspectives and is a multi-dimensional construct. They find that the 20 items used in RQ are consistently loaded onto two factors: emotional appeal and cognitive components of performance.

Ponzi et al. (2011) developed RepTrak Pulse, a relatively short-form and simplified measure of corporate reputation. This is a reflective measure consisting of four items: company feeling (i.e., I have a good feeling about the company), admire and respect (i.e., I admire and respect the company), and company confidence (i.e., I trust the company) and the fourth item to rate the company's overall reputation (i.e., the company has a good overall reputation), eliciting the company's overall emotional appeal to the respondents. RepTrak Pulse captures emotional perceptions that are distinct from cognitive conceptions based on performance indicators, such as financial performance, better

[37] The concept of corporate reputation used in RQ is 'a collective construct that reflect the cumulative perceptions of multiple stakeholders about a company's performance' (Ponzi et al., 2011).

working environments, quality of product or services, etc., making it more unbiased and robust against distorting halo effects. Bergh et al. (2010) also support that a reflective measurement is more suitable for measuring unobservable, intangible resources, like corporate reputation. Some other corporation reputation rating scales include the work of Schwaiger (2004), Helm (2005), Walsh and Beatty (2007), Walsh et al. (2009), and Highhouse et al. (2009).

4.3 Corporate reputation risk

While strong corporate reputation may bring superior financial performance and sustainable competitive advantages, poor or damaged reputation may result in significant disadvantages, such as reduced revenues, decreased ability to attract financial capital, or reduced appeal to current and potential employees which may lead to reduced economic returns and shareholder value (Fombrun et al., 2000). For example, a customer who learns about a product safety recall may be reluctant to purchase that brand of product, impacting the achievement of the company's sales target. If a construction company were sued for cracks in the newly constructed building walls, its reputation may be affected to the point of lost profits, lost clients, and even bankruptcy. Damage to the organization's reputation may increase the organization's overall business risk exposure level to indicate the possibility that the intended performance targets or business objectives are not achieved.

More formally, Rayner (2004) states that all risk sources that impact the corporate reputation should be grouped together as reputation risk, rather than attempting more nimble categorization. Similarly, Dowling (2006) asserts that all enterprise-wide risks are leading indicators of corporate reputation risk. Reputations are built from inside the

organization creating: good values and culture, quality products and services, or superior customer value propositions.

Dowling (2006) also asserts that misalignment of the organization's reality and social expectations is a driver of corporate reputation risk. Larkin (2002) also suggests that corporate reputation is rooted in a changing society which may involve rising shareholder expectations about the social responsibility and shifting trust in companies and their leaders.

Eccles et al. (2007) also emphasize the importance of meeting stakeholder expectations in managing corporate reputation risk. They state that there are three determinants of corporate reputation. First, the reputation-reality gap concerns whether expectations about the company expectation are more positive than its true characteristics. For example, BP's "Beyond Petroleum" advertising campaign and expensive initiatives to promote its alternative-energy business had cultivated a good reputation during 2003 and 2004, but when several major accidents happened in 2005 and 2006, its reputation got damaged significantly.[38] Second, stakeholders' changing beliefs and expectations can widen this reputation-reality gap, increasing the reputation risk for those companies that cannot keep pace. Third, weak internal coordination may also increase reputation risk. In other words, when one group creates expectations and another fails to meet them, the company's reputation may suffer. For example, the marketing department may promote new products or services before the manufacturing department can begin production. Subsequent launch delays would damage reputation.

[38] BP's Sinking Image cited in Eccles et al.(2007)

The literature reveals that corporate reputation suffers when stakeholders' expectations are not met. Corporate reputation risk may encompass all sources of risks or events that impact the reputation and typically arises when the organization fails to meet stakeholders' expectations. Therefore, it is important to understand the stakeholders' expectations, recognize when they change, and consistently provide good value and culture, quality products and services, or superior customer value propositions for maintaining strong and sustainable reputation (Rayner, 2004; Fombrun et al., 2000; Dowling, 2006; Eccles et al., 2007).

4.3.1 Assessing Corporate Reputation Risk Level using KRIs

Most corporate reputation measures are based on ratings of companies computed from polls, surveys, and interviews which are conducted at a certain point in time. Such periodic corporate reputation measures would only provide a snapshot of the organization's reputation and not be effective for the risk based auditor to detect changes in a timely manner. Reputation risk should be monitored and assessed in continuously, capturing significant changes and reflecting them in subsequent audit procedures. The KRI based CRMA methodology may provide a new approach to achieving such continuous assessment and monitoring of the organization's reputation risk.

4.3.1.1 Identification of corporate reputation risk

As discussed in the previous chapter, the proposed CRMA methodology identifies the organization's risks by three categories: process risks, environmental risks, and Black Swans. Process risks arise from failed internal processes, people, or systems, which may include rogue trader, senior management scandals or fraud, failures of critical business processes, improper strategies, information security breaches, etc. Environment risks include all risks that originate from the organization's external environment, such as

bankruptcy of suppliers, intense competition, product obsolescence, new regulations, unstable politics, etc. Black swans are extremely rare, but could happen and create huge losses (‘low probability, high impact’) (Taleb et al., 2009). Such black swan risk events may be identified through ‘reasoned imagination’ with the signals or pre-cursors to the risk events (Pate-Cornell, 2012). This three-risk category framework used in the proposed CRMA methodology would help the auditor to acknowledge the organization’s all potential major risk events.

All events (process, environmental, or black swan) that could affect the organization’s ability to meet stakeholder expectations may drive their reputation risk exposure. The sources of the organization’s reputation risk may be identified across all three risk categories used in the proposed CRMA methodology. For example, a bank’s poor liquidity management policies and process identified as their process risk may also drive their reputation risk because such poor liquidity risk management may negatively appeal to their creditors, thus the bank’s reputation may suffer. In this case, the reputation risk originates from the organization’s internal processes.

An organization’s reputation risk may be driven by their external environment. For example, a third party partner of the organization operating in a different country could be involved in unlawful practices, such as the use of child labor or bribes, which would affect the organization’s reputation. This is an example of the external environment increasing reputation risk. The less control a company has over its partners, the greater its exposure to corporate reputation risk.

Black swan events may also impact the organization's reputation significantly. For example, the unprecedented financial crisis in 2007 (Taylor and Williams, 2008) caused a loss of investor and creditor confidence in financial institutions.

4.3.1.2 Selecting KRIs for Corporate Reputation Risk

The Global Reputation Risk survey[39] conducted by Deloitte in 2014 found that 88% of respondents consider reputation risk as 'more important' and explicitly focus on managing their reputation risk. Respondents who have experienced negative reputation events previously reveal that the most impacted areas were revenue, loss of brand value, and regulatory investigation. More than 50% of companies say that they plan to invest in technology such as analytical and brand monitoring tools to improve their capabilities for managing reputation risk. Companies are increasingly aware of the importance of reputation risk management and strive to mitigate their exposure.

The proposed CRMA methodology utilizes KRIs to assess the organization's risk exposure levels in a continuous manner. As we discussed, under the CRMA methodology, multiple KRIs (leading indicators and CEIs) are combined as an index to better reflect multiple signals of a given risk and assess its exposure level. By monitoring leading indicators, the auditor may be able to estimate how likely the given risk will materialize and impact audit risk. By tracking CEIs, the auditor may confirm that an event has occurred and determine its effects on audit risk. Combined, these indicator types would provide more comprehensive information about the given risk. As such, the proposed CRMA methodology integrates leading indicators and CEIs into an index value to better assess each given risk's exposure level quantitatively. Above all, since the proposed

[39] The survey was conducted by Deloitte and Forbes Insights and subject on more than 300 executives from all major industry and geographic region.

CRMA methodology uses data driven KRIs, it would be more feasible to continuously assess the organization's risk exposure levels and recognize significant changes in a more real time manner.

Reputation risk can be driven by any event that increases the likelihood of failure to achieve the organization's expected goals or objectives (Rayner, 2004). For example, heightened cyber-attack risk exposure may increase the likelihood that their customers' private information could be stolen by hackers, indicating a high reputation risk.

As for CEIs for an organization's reputation risk, there could be two types of indicators: stakeholders' current emotional perceptions of the organization, and the performance indicators affected by the organization's reputation, such as daily or weekly sales figures or stock price. First, corporate reputation is the collective perceptions of the organization held by their stakeholders (Fombrun and van Riel, 1997; Ponzi et al., 2011). The data representing people's perceptions may include positive or negative sentiments expressed in social media, news, or blog websites. Second, performance indicators may represent the lagging effects of the organization's reputation. Such performance indicators may include sales or stock prices, number of unfavorable customer reviews and news, etc. These CEIs would represent circumstances or situations appeared when the organization's reputational damage occurred. In other words, the CEIs for the organization's reputation risk would confirm the organization's materialized reputational damage. For example, suppose an insurance company received a cyber-attack and lost thousands of its customers' private information. CEIs (e.g. emotional sentiments expressed in the news or comments in the social media websites) would provide information about the effects of this event on the organization's reputation. Performance

indicators (e.g. stock prices, decreased sales, etc.) would also represent the lagging effects of such risk event on the organization's reputation. Monitoring trends in such CEIs would help to catch changes in the organization's reputation and detect their damaged reputation in real time.

Conventional corporate reputation scales, such as AMAC or RQ, are CEIs based on ex-post viewpoints. However, they are mostly questionnaire survey or interview based instruments and annually published periodicals (Ponzi et al., 2011; Casado et al., 2014). Such static and periodic information may not provide timely information to detect changes in the organization's reputation in a real time manner. Real-time KRIs would be needed for continuous assessment of corporate reputation risk under the proposed CRMA methodology. We suggest a following framework to identify the leading indicators and CEIs (Table 10)

	Data for KRIs of corporate reputation risk
Leading Indicators	• Current exposure levels of other risks (i.e., high liquidity risk, high operational risk, high fraud risk, etc. These risks increase the risk of failure in the related areas, but also may elevate the corporate reputation risk as secondary consequences).
Confirmatory Event Indicators (CEIs)	• Current emotional perception held by the stakeholders and performance indicators affected by changes in the corporate reputation (i.e., trends in sales or stock prices)

Table 10 Relevant KRIs for corporate reputation risk

4.3.1.3 Measuring selected KRIs

The proposed CRMA methodology aims to collect and monitor relevant KRIs in a continuous manner. The proposed methodology assumes that CRMA takes advantage of the auditor's continuous data monitoring and analysis layer (i.e., MCL, Vasarhelyi et al., 2004) connected to the organization's automated and integrated information systems in

extracting and analyzing business process data and performance metrics, as well as external data resources to monitor and assess relevant KRIs. For example, suppose the number of unresolved customer complaints is used to monitor the organization's operational risk exposure level. This KRI may be computed in the CA auditor's MCL module which automatically and regularly accesses the organization's customer relation management (CRM) and subtracts total number of customer complaints resolved from the number received, monitoring the relevant KRI continuously.

Current performance indicators such as stock price or sales figures may be obtainable from the organization's internal business processes and performance metrics, such as daily or weekly sales figures or from external websites such as Yahoo Finance or Google Finance. However, the stakeholders' current perceptions about the organization may not be as easily obtained. To obtain such data to assess the stakeholders' current emotional perceptions, the CRMA auditor may want to analyze social media and extract the sentiments embedded in the public's emotion or attitudes toward the organization. These resources may help to develop a KRI to catch the public's sentiments and monitor changes in the organization's reputation as a CEI.

4.3.1.4 Description of the proposed KRI

We propose a KRI which would assess the effect of the organization's risk on their reputation. The proposed KRI measures the degree of negative emotion or perception of the organization expressed by comments posted on social media. These channels are easy to use, real-time, and contain public opinion on various topics that range from products and services, to environment and politics, to technology and entertainment (Asur and Huberman, 2008). The sentiments reflected in social media websites may reveal changes

in the public's perceptions of an organization in real time, providing useful information to evaluate an organization's current reputation level.

For example, a persistent long trend of negative sentiments expressed on social media after a risk event may indicate a sign of the organization's damaged reputation, thus confirming their reputation damage. A KRI which provides the information about public perception after a risk event in real time may improve the auditor's ability to recognize change in an organization's reputation affected by the risk event. Hence, we propose using social media data as a CEI to measure the organization's current reputation level and confirm the occurrence of the reputation damage as follows:

$$Social\ media\ KRI = \frac{Number\ of\ Negative\ posts}{Number\ of\ Negative\ posts + \ Number\ of\ Postive\ posts}$$

4.4 Sentiment Analysis on Twitter Data

We demonstrate the present KRI by using Twitter messages (or 'tweets') posted during immediately after two real risk events occurred: Purina's lawsuit for selling harmful dog food (CNN, 2015) and Starbucks' 'Race Together' campaign (WSJ, 2015). We downloaded relevant tweets through the Twitter API and conducted sentiment analysis to classify them into positive, negative, and neutral polarity categories to compute the present KRI.

Many researchers use Twitter data for various purposes. For example, some researchers studied the effectiveness of Twitter as a social and information sharing platform (Kwak et al, 2010; Huges and Palen, 2009; Herring and Honeycutt, 2009). Others study text mining techniques for tweets to find better automatic classification algorithms that use their polarity types (Go et al., 2009; Thelwall et al., 2010, 2011; Pang and Lee, 2005). Many

researchers also examine whether the sentiments expressed by tweets can be used to predict the future of various subjects including movie ticket sales, stock performance, or elections (Asur and Huberman, 2010; Rui et al., 2013; Wu et al., 2010; Gilbert and Karahalios, 2010). We provide the background of Twitter and related literature in the following sections.

4.4.1 Twitter for social and information sharing purpose

Twitter is a micro-blogging and social network website where the users post short status updates on various topics and share them with other users (Go et al., 2009; Thelwall et al., 2011). Twitter users can post messages (called 'tweets') containing up to 140 characters. A Twitter user can search for tweets that concern a particular topic by its hashtag ('#') and comment on that particular topic. A Twitter user can follow other users and read and respond to messages by directing comments to them with '@' symbol.

The potential for information dissemination and sharing through Twitter is significant. Kwak et al. (2010) documented from their analysis of 106 million tweets that if a tweet is retweeted, it can be expected to reach an average of 1000 users. Huges and Palen (2009) discovered that an important event triggers more tweets and suggested that Twitter has information diffusion.

Also some researchers find that Twitter is also effective for conversations and collaborations. Honeycutt and Herring (2009) report that the '@' feature facilitates the conversational uses of Twitter. Boyed et al. (2010) also argue that Twitter users post their messages for conversational purposes rather than just information broadcasting purpose based on the high use of '@' identified in their 720,000 tweet sample.

People comment and read tweets not only to share information, but also to communicate and collaborate with other users by responding to their messages or external events (Thelwall et al., 2011). Seeking and responding to external information are collectively referred to as information behaviors (Wilson, 2000). It is known that such information behaviors always involve affective components (Thelwall et al., 2011; Nahl and Bilal, 2007). Tweets responding to various subject matters may convey their affective or emotional status regarding given subject matters. Therefore, we use tweets to as a KRI that measures the public's perception.

4.4.2 Real time access to Twitter data

Twitter messages are available to the public through its API (Application Programming Interface)[40]. The Twitter API provides the interface between the developers and Twitter data. Developers may search for and download tweets by various parameters such as words, phrase, hashtags, users names, language used, or location.

There are two types of APIs available: Rest API and Streaming API. They both utilize HTTP based requests such as GET, POST, and DELETE. Rest API provides access to read and write specific Twitter data such as user profiles, messages, follower information etc. The Streaming API provides real-time access to monitor and process the Twitter data. It gives real-time stream of Twitter data. Data from both APIs are stored in either XML or JSON format.

However, the amount of tweets that can be downloaded at no charge is limited. Currently, only tweets up to ten days old can be accessed for Rest APIs, and less than 1% of total tweets can be downloaded through Streaming APIs. Older data is available for purchase

[40]https://dev.Twitter.com/overview/documentation

from third party providers such as Gnip[41]. DuVander (2012) reports that over 3 billion tweets and 15 billion API requests are generated on daily basis. Such a large number of API requests may indicate that Twitter is a premier means of social media analytics (Abbasi et al., 2014).

Bifet and Frank (2010) describe Twitter as a 'what's-happening-right-now' tool that allows interested parties to follow each other's thoughts or comments on the events or news about their lives in almost real-time. Terpstra et al. (2012) document that people use Twitter messages to share information about crises such as floods, earthquakes, hurricanes, or other natural hazards and to express their opinions and feelings in real time. Given that Twitter users post in real time, their messages would be a good source to quickly gauge people's emotional state on given subject matter.

4.4.3 Sentiment expressed in Twitter messages

Many researchers investigate whether the public's sentiments reflected in tweets can be used to predict the future. Examples include political elections (Tumasjan et al., 2010; O'Connor et al., 2010; Diakopoulos and Shamma, 2010), stock market indicators (Zhang et al., 2010; Gilbert and Karahalios, 2010; Bollen et al., 2009, 2011; Smaliovic et al., 2014), and box-office revenues (Asur and Huberman, 2010; Shi and Whinston, 2013). Tumasjan et al. (2010) analyzed over 100,000 tweets and found that Twitter message volume was a good predictor of the 2009 German election. Zhang et al (2010) analyzed the sentiments in tweets and showed that negative sentiments are negatively correlated with stock market indices such as Dow Jones, NASDAQ, and S&P 500. Shi and Whinston (2013) collected over 4 million tweets mentioning 63 movies and compared the

[41] https://gnip.com/sources/Twitter/

tweets with box office revenues. They found that positive tweets are associated with higher sales, while negative tweets are associated with lower sales.

4.4.3.1 Sentiment analysis

Sentiment analysis[42] involves extracting opinions from unstructured human-authored documents such as reviews or blogs (Pang and Lee, 2008). It typically entails two or three steps. First, the input text is evaluated for subjective content. Second, subjective texts are analyzed and labeled by either positive or negative polarity (Thelwall et al., 2010, Pang and Lee, 2008).

Sentiment analysis has traditionally focused on lengthy texts in the context of reviews, such as movie or product reviews (Pang and Lee, 2008; Go et al., 2009). Classification is a fundamental technology in many current opinion-mining and sentiment analysis applications (Pang and Lee, 2008). Sentiment classification in general refers to the binary classification which is the "task of labeling an opinionated document as expressing either an overall positive or an overall negative opinion" (Pang and Lee, 2008, p.25). However, sentiment classification can also refer to alternative binary categorization, multi-class categorization, regression, and/or ranking (Pang and Lee, 2008). One example is classifying a news article as containing good or bad news. Categorizing sentiment-based product reviews to extract pro and con content and identifying reasons for an opinion could be also considered as an application of sentiment classification (Kim and Hovy, 2006; Pang and Lee, 2008). Multi-class categorization, regression, or ranking may include determining the text units with respect to a multi-point scale (degree of positivity) or classifying them into positive, neutral, and negative classes (strength of opinion).

[42] It is also known as opinion mining or subjectivity analysis (Pang and lee,2008)

Neutral class could be a mixture of positive and negative language, or a lack of opinion (Pang and Lee, 2008). However, Cabral and Hortacsu (2004) report that neutral comments in e-bay feedback systems are perceived by users to be much closer to negative feedback than positive, suggesting that neutral comments may not necessarily indicate a mid-point between positive and negative comments.

The algorithms of sentiment analysis often use machine learning techniques to identify general features associated with positive and negative sentiment classes for the given texts (Thelwall et al., 2010). Such features may include particular characteristics such as emoticons, repeated punctuation, and parts of speech (or n-grams) which represent the frequency of occurrence of all n consecutive words (Thelwall et al., 2010). Other sentiment analysis approaches include lexicon based and linguistic approach; the former utilizes a dictionary of positive and negative words[43] and counts their frequency text to determine polarity, and the latter uses compositional semantics rules to determine the polarity of an expression (Thelwall et al, 2010).

4.4.3.2 Tools for sentiment analysis

There are many tools developed to analyze sentiments in short informal social media text. Abbasi et al. (2014) grouped 20 such tools into two categories: stand-alone tools[44] and workbench tools[45]. Stand-alone tools can directly categorize unlabeled texts into positive,

[43] There are number of sentiment words dictionaries developed by researchers such as OpinionFinder (Wilson et al.), Affective Norms for English Words (Bradley and Lang),SentiWordNet (Baccianella et al.)

[44] They include uClassify, ChatterBox, Sentiment140 (Go et al. 2009), Textalytics, Intridea, AiApplied, ViralHeat, Lymbix, Anonymous (the authors do not disclose its name), SentimentAnalyzer, TextProcessing, Semantria, SentiStrength (Thelwall et al., 2010), MLAnalyzer, and Repustate.

[45] They evaluated total 5 workbench tools: LightSide, BPEF, EWGA, FRN, and a word n-gram baseline run using the text processing extension in RapidMiner

negative, or neutral polarity. These tools can be used on an API basis or downloaded as a desktop application. The primary advantage of such tools is ease of use, but a lack of domain-specificity may degrade performance (Abbasi et al., 2014). In contrast, workbench tools use a supervised learning model and therefore require labeled training data. They involve extensive parameter tuning and validation, but may incorporate domain specific knowledge.

4.4.3.3 Classifying Twitter message into its polarity

There are two popular sentiment analysis tools developed by academic researchers: Sentiment140 (Go et al., 2009) and SentiStrength (Thelwall et al., 2010). For the first time, Go et al. (2009) classified tweets by sentiment polarity. They automatically identify positive and negative tweets by taking advantage of tweets with emoticons rather than conducting labor intensive manual coding. For example, tweets with :), :-), :), :D, or =) are labeled as positive, and tweets with :(, :-(, or :(are negative. They collected total 1.6 million negative and positive tweets from various domains and successfully trained machine learning classifiers such as naïve Bayes, maximum entropy, and support vector machines.

Whereas Go et al. (2009) uses machine learning based methods and focuses on classifying texts into positive and negative polarity, Thelwall et al. (2010) developed a lexicon based algorithm named SentiStrength to extract sentiment strength (both positive and negative) from text. They developed a dictionary of positive and negative words for their sentiment strength levels ranging from 2 (least) to 5 (high or extreme) from 2,600 manually labeled MySpace comments. The dictionary includes negative and positive

sentiment words, emoticons, phrases, and other textual methods of expressing sentiment (i.e., repeated letters (e.g. “a loooong time”) or punctuation (e.g. “Hi!!!”)). Using this dictionary, SentiStrength scores on a scale of 1 (no sentiment) to 5 (very strong positive sentiment) for positive and -1 (no sentiment) to -5 (very strong negative sentiment) for negative polarity simultaneously. For example, the algorithm would assign ‘I love music’ a score 4 for positive and -1 for negative sentiment. For another case, the algorithm would assign ‘I hate Paul but encourage him’ a positive sentiment strength score 2 and a negative sentiment strength score -4[46].

However the overall polarity of the given text can be determined by aggregating positive and negative strength scores (Taboada et al., 2011; Thelwall et al., 2012; Bravo-Marquez et al., 2013). For example, ‘I love music’ is assigned a 4 positive and -1 negative score. Thus, its overall polarity would be positive, since the aggregated score is 3 which is greater than 1 (no sentiment). On the other hand, if the combined score is less than -1, it would be considered negative. For example ‘I hate Paul, but encourage him’ would be rated as a negative text since its positive score is 2 and its negative score is -4, thus its combined strength score is -2.

Normally the sentiment analysis first involves filtering non-subjective texts (a score of -1, 0, or 1). The remaining subjective corpus is analyzed for sentiments. For such reason, in general, sentiment analysis starts with extracting subjective documents from the corpus (Pang and Lee, 2008; Thelwall, 2011)

[46] SentiStrengh algorithm can be available for test at http://sentistrength.wlv.ac.uk/#Test , and more tutorial slides can be found at http://sentistrength.wlv.ac.uk/#Download

4.4.3.4 Domain dependency

Pang and Lee (2008) note that "sentiment and subjectivity are quite context-sensitive and at a coarser granularity, quite domain dependent (in spite of the fact that the general notion of positive and negative opinions is fairly consistent across different domains)" (p. 21). This implies that the same expression may signify a different sentiment in different domains. For example, "go read the book" may indicate positive sentiment for book reviews, but negative sentiment for movie reviews (Pang and Lee, 2008); "unpredictable" is a positive expression for a movie, but negative for a car's steering abilities (Turney, 2002). Sentiment classifiers trained on one domain may not be accurate for another domain (Pang and Lee, 2008). Sentiment classification differs from domain to domain, suggesting that building a domain specific classifier is important to avoid domain dependency (Owsley et al.,2006, Pang and Lee, 2008, Read, 2005).

4.5 Case Studies

The proposed KRI measures the proportion of negative comments to the total subjective comments about an organization posted on social media for a given time period (i.e., hourly or daily). Continuous monitoring of the present KRI would quickly reveal when the public's perceptions of an organization turn negative, thus help to detect the organization's reputational damage and assess the potential adverse impacts on their business operations due to the damaged reputation in a timely manner. As such, the present KRI may be used as a CEI to recognize the organization's materialized reputation risk. To demonstrate the proposed KRI, we use two real reputational risk events and the tweets posted when these events occurred. We perform a sentiment analysis on these

tweets classifying them into positive, negative, and neutral polarity to compute the present KRI.

4.5.1 Methodology

We used supervised machine learning to classify tweets into positive, negative or neutral polarity. Supervised leaning algorithms are trained to learn sentiment classification rules from pre-classified training data, and then the algorithms are applied to classify test data (Das and Chen, 2007). The training data we used containing 11,820 short informal texts[47] from various social media and forum web sites including Twitter, MySpace, YouTube, BBC, Digg, and Runner's World. This database was used by Thelwall et al. (2012) for testing their new sentiment classification algorithm (SentiStrengh2, Thelwall et al., 2012). Thelwall et al. (2012) used three independent coders to manually label each text in this data set and used it to test their new algorithm. The each text was classified in terms of its positive and negative sentiment simultaneously on a scale of 1 to 5 (positive sentiment) and -1 to -5 (negative sentiment). For example, "Love your pics! Thanks for the add!! :)" is rated as 4 positive and -1 negative (i.e., no negative sentiment). On the other hand, objective text such as "We know how it works" is rated as positive 1 and negative -1, which means that there is neither positive sentiment nor negative sentiment.

We filtered text with fewer than 20 or more than 150 characters to only incorporate the text with the length of a typical tweet into our training database, leaving 5973 texts. We cleaned them to remove stopwords and heading and trailing white space, punctuation, and numbers. We stemmed all words and made them lower case. We used R's 'tm' package (Feinerer, 2015) for such data preprocessing and filtering.

[47] This dataset is available at http://sentistrength.wlv.ac.uk/#Download

To label the polarity of each text in the training data set, we aggregated its positive and negative sentiment strength scores. If the combined sentiment strength score of a given text is greater than 1, we label it as positive and code it as 1. If it is less than -1, we label it as negative and code it as -1. If the aggregated score of a given text falls among 1, 0, and -1, whose means no sentiment, we label it as neutral and code it as 0. Once the aggregated score is computed for every text in the training dataset, three variables (positive score, negative score, and text) of the original dataset are reduced to two (polarity code: 1, 0, or -1, and text).

With this training set, we attempted 3 supervised learning algorithms: naïve Bayes, random forest, and SVM (Support Vector Machine) to train classifiers of positive, negative, and neutral sentiment polarities. We used R packages 'klaR'[48], 'randomForest' [49][50], and 'e1071'[51] (Dimitriadou et al., 2005) for naïve Bayes, random forest, and SVM respectively.

As shown in Table 11, on 10 fold cross-validation data sets and with a dictionary size of 1,434, the random forest algorithm performs best and results in the highest overall accuracy rate among these three supervised learning algorithms. It performs particularly well when classifying negative polarity. Since the proposed KRI measures the proportion of negative subjective messages to the total number of subjective messages, we chose to use random forest in classifying the collected tweets for each reputational risk event.

[48] https://cran.r-project.org/web/packages/klaR/klaR.pdf
[49] https://cran.r-project.org/web/packages/randomForest/randomForest.pdf
[50] http://www.bios.unc.edu/~dzeng/BIOS740/randomforest.pdf
[51] https://cran.r-project.org/web/packages/e1071/e1071.pdf

	Positive	Neutral	Negative	Average
Naïve Bayes	50%	50%	50%	50%
SVM (Linear)	70%	62%	62%	65%
Random forest	71%	63%	67%	67%

Table 11 Accuracy rates of three selected algorithms on three sentiment classes

In the following section, we present each reputational risk event we analyzed and the results from our sentiment analysis to measure the proposed KRI and related findings.

4.5.2 Case 1: Purina lawsuit

Purina[52] is a US based subsidiary company of Nestle Corporation, which produces and sells pet care products, mainly food and snacks, for dogs and cats. In February 2015, major news media channel such as CNN, Fox, and NBC broke news about lawsuits against Purina for selling harmful dog food that allegedly resulted in the "serious illness and death of thousands of dogs" (CNN, 2015). Although Purina initially denied the accusation, it was possible that the Purina's brand image and its reputation were going to be damaged. Therefore, we chose this reputational event of Purina to see if the proposed KRI would offer information to understand how people's perceptions of Purina were affected by this reputational event. To that end, we classified tweets mentioning Purina posted immediately following this news.

4.5.2.1 Data

We collected tweets mentioning 'Purina' through Twitter's Rest API over the time period between 2/20/15 and 2/27/15[53]. Since the news about the lawsuit appeared on 2/24, the tweets posted during such time period would reflect the public's emotions before and

[52] www.purina.com,

[53] The earliest tweet collected was time stamped as 2/20, 15:00-16:00, US EST and the last tweet was recorded at 2/27, 19:00-20:00 US EST.

after the news broke. 1,002 tweets were collected. We preprocessed the data before feeding it to our classifiers by removing stopwords, heading and trailing white spaces, and punctuation. We also stemmed the corpus and converted it to lower case.

4.5.2.2 Results

Figures 13,14, and 15 below show the total number of negative, neutral, and positive tweets per hour for the time period between 2/20 and 2/27 respectively. Figure 16 shows the total number of positive, neutral and negative tweets per day for the same time period. Figure 17 presents the total number of tweets combined with positive, neutral, and negative tweets.

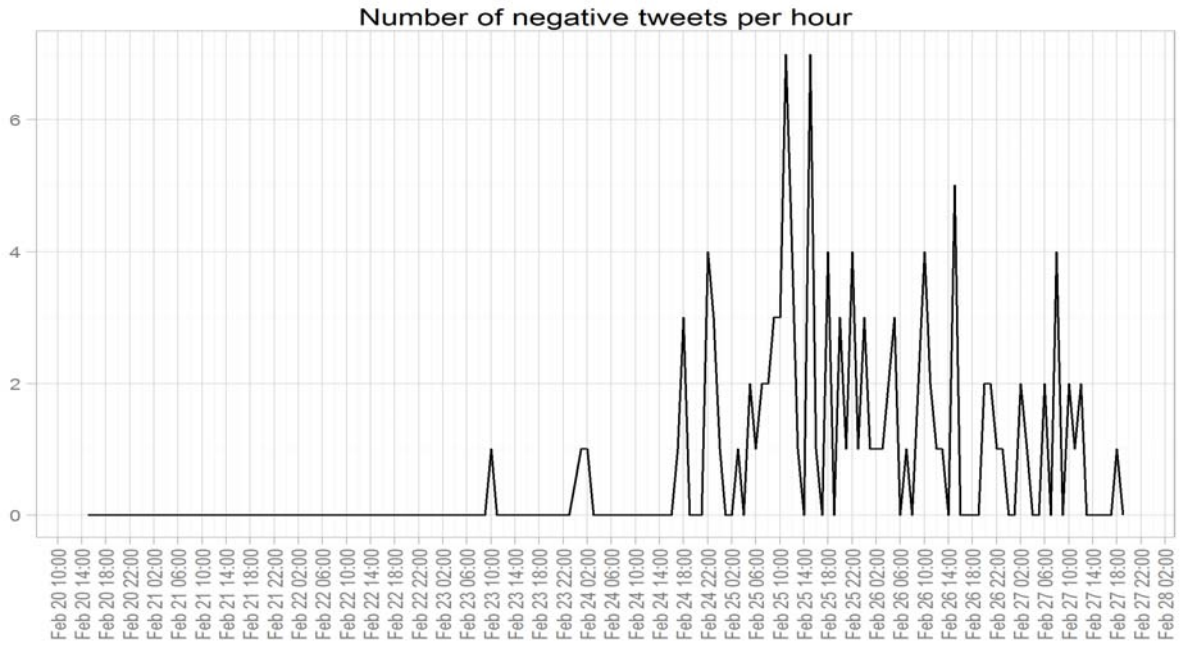

Figure 13 Number of negative tweets per hour for the time period between 2/20/2015 – 2/27/2015 (Purina)

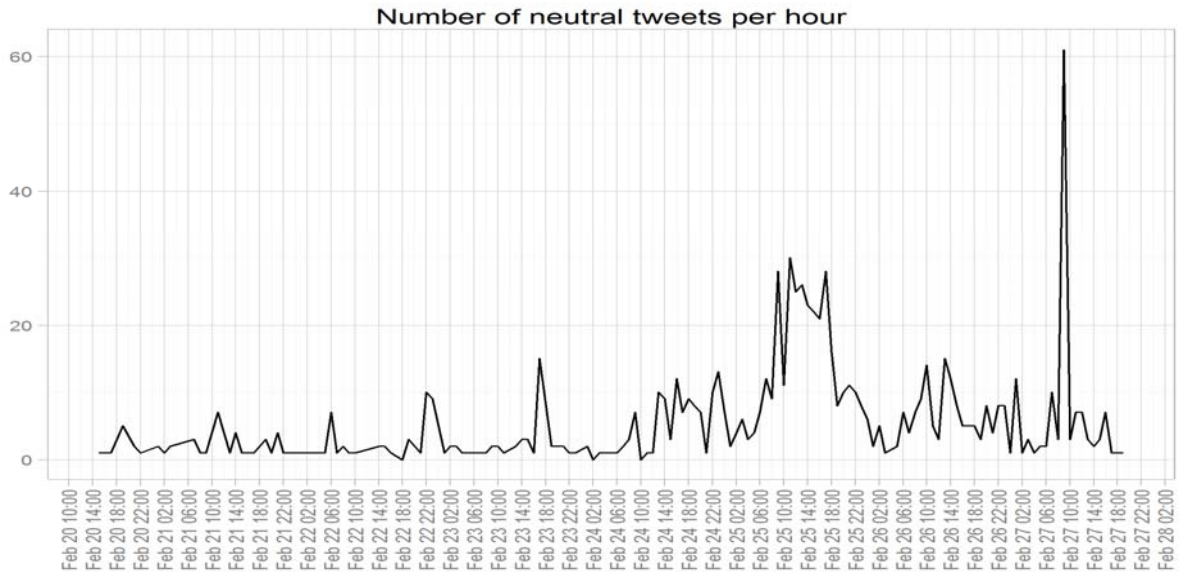

Figure 14 Number of neutral tweets per hour for the time period between 2/20/2015 – 2/27/2015 (Purina)

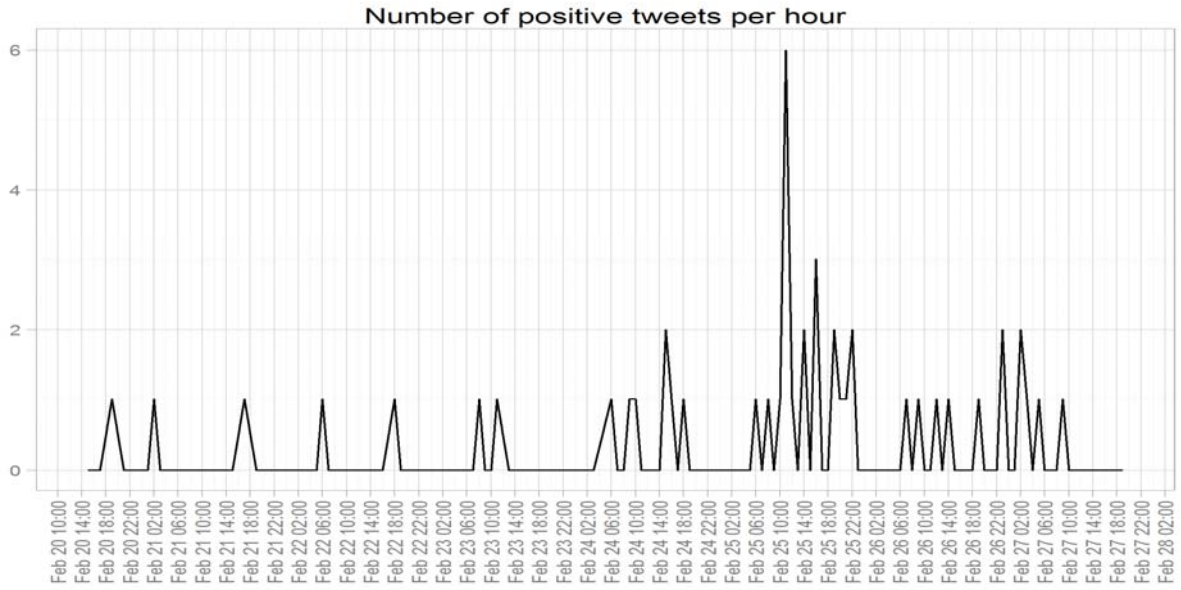

Figure 15 Number of positive tweets per hour for the time period between 2/20/2015 – 2/27/2015 (Purina)

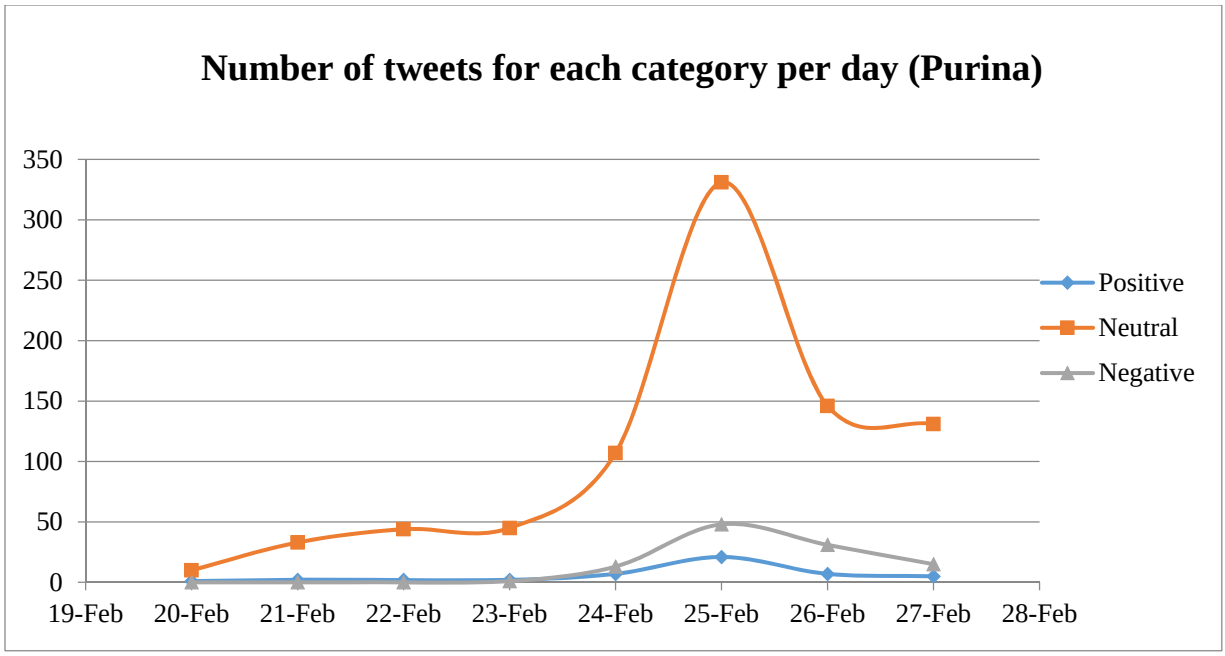

Figure 16 Total numbers of tweets of each category per day for the time period between 2/20/2015 – 2/27/2015 (Purina)

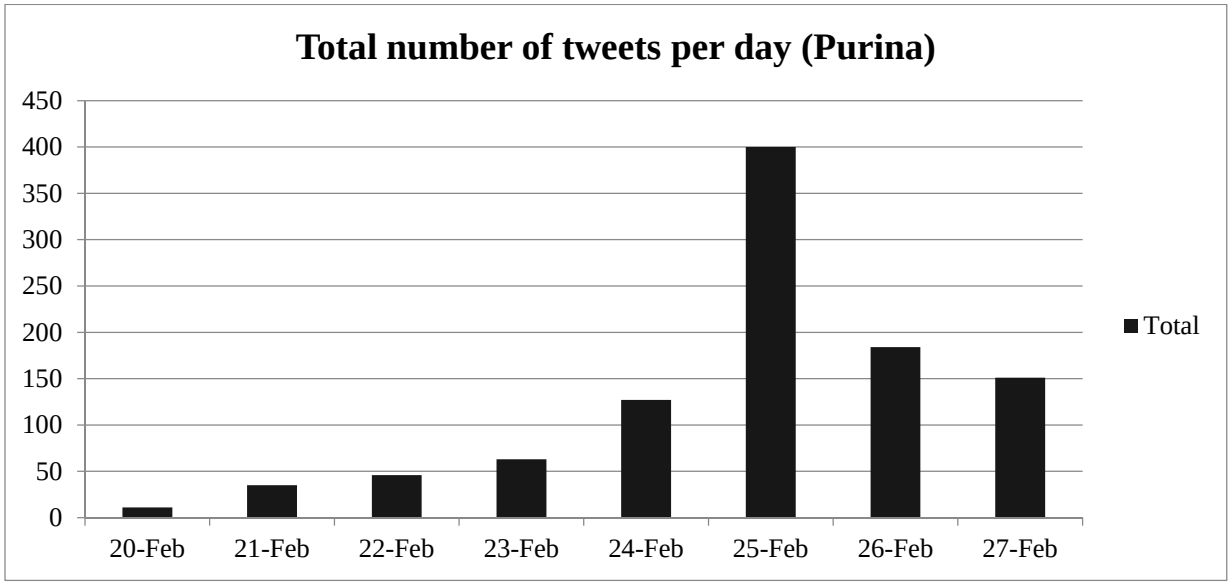

Figure 17 Total number of tweets per each day for the time period between 2/20/2015 – 2/27/2015 (Purina)

As shown in the Figure 17, there was a remarkable increase in the total number of tweets posted when the news about the lawsuit appeared (2/24). This indicates that the news

attracted attention and may have affected perceptions about the company. However, as Figure 16 reveals, most of the tweets posted during such time are labeled as neutral. This may indicate that there had been many objective tweet messages posted when the news initially appeared on 2/24, which would make sense as many news media or other users would have used Twitter as a means of conveying the news about the case.

In order to see how much users affectively (emotionally) responded to the Purina's lawsuit event, we looked at the ratio of total affective comments or messages (i.e., positive tweets + negative tweets) to the total number of tweets (positive + neutral + negative tweets) posted in a given day.

Figure 18 shows such rate of the total number of subjective tweets to total number of tweets posted per day during the time period between 2/20/2015 – 2/27/2015 along with the values of the proposed KRI for the same time period. As shown in Figure 16, the number of subjective tweets increased during the time, particularly when the news was spread out. But the rate of subjective message rates increased by about 10% during such time. This fact may have been influenced by the relatively higher number of neutral tweets posted during the same time frame.

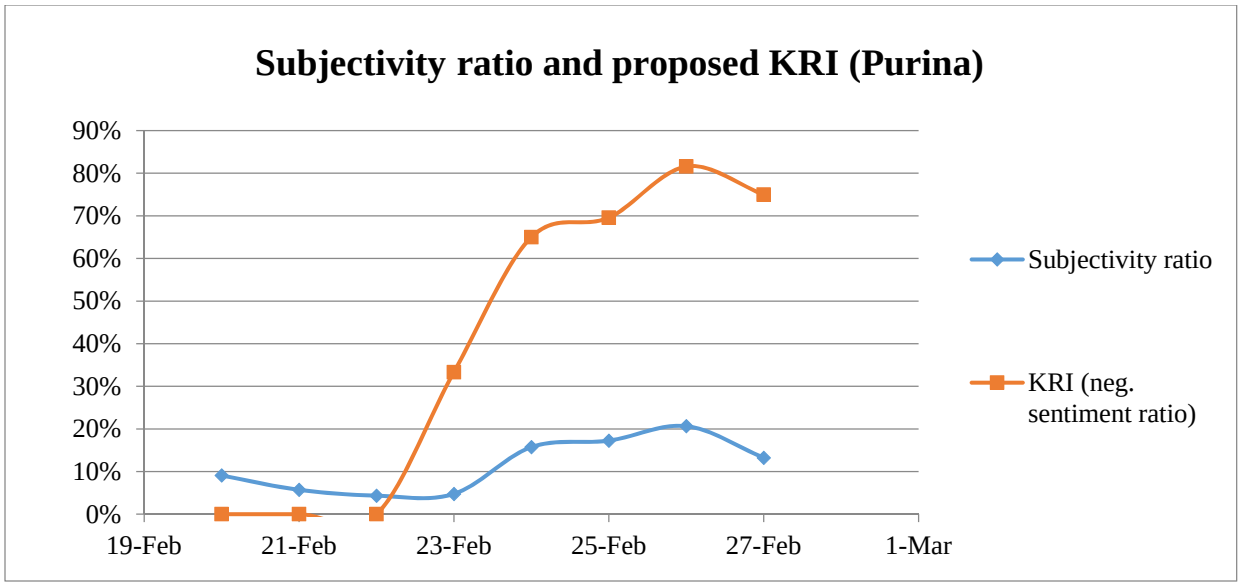

Figure 18 Ratio of subjective tweets to total number of tweets vs. the ratio of negative tweets to the total subjective tweets (Purina)

As discussed before, we propose that a KRI which could measure the current level of people's negative perceptions of the organization's may help the risk based auditor to assess the organization's reputation more rapidly. Applying this KRI in Purina's case, which can be measured by dividing negative tweets posted in a given day by the total number of subjective tweets (i.e., positive + negative tweets), we observe that it detects the significant increases in the negative tweets posted during the time the Purina lawsuit case started to appear in the mass media. In the period before the lawsuit, there were no tweets labeled as negative, but as shown Figure 18, after the news came out on 2/23, the rate soared from 0% to 82% and remained high. The event significantly affected Purina's reputation as negative perceptions linger after the event occurred. Such information about the lingering effect of the risk event represented by the proposed KRI may help the auditor to recognize changes in the organization's reputation and to prepare more

proactive audit plans that deal with the organization's emerging significant reputational damage.

4.5.3 Case 2: "Race Together"

Starbucks Corp. initiated the social campaign named "Race Together" in March 16, 2015. The motivation of this campaign was to help improve racial tensions. The company considered its new campaign as "an opportunity to begin to re-examine how we can create a more empathetic and inclusive society—one conversation at a time" (WSJ, 2015). As part of this campaign, the employees of Starbucks (baristas) were asked to write "Race Together" on cups given to customers and encouraged to engage them in conversations about race relations.

However, the company faced strong criticism over this campaign for several reasons. Some people criticize the inappropriateness of prompting customers to engage in conversations about delicate racial issues at a place where they come to get a quick coffee on the run. Others saw it as a marketing ploy. The company finally halted the campaign two weeks later, on March 23, 2015.

The high profile of this campaign received attention from mass media and commentators. This event is a reputational risk event as it received strong criticisms which may affect people's affective perception of the company and its reputation.

4.5.3.1 Data

We collected 20,000 tweets mentioning 'Starbucks' or 'Race Together' posted from 3/22/2015 to 3/28/2015. We used Twitter's Rest API to download relevant data. Twitter only provides a limited amount of historical tweets, and the earliest date and time we could go back was 3/22/2015, 22:00-23:00 US EST. The latest tweet was recorded at

3/28/2015 16:00 US EST. These tweets were posted after the company made the decision to cease this controversial campaign. The proposed KRI would catch how this decision affected people's perceptions of the company, helping to assess the organization's current reputation affected by that decision.

4.5.3.2 Results

Similar to the Purina analysis, we classified tweets mentioning 'Starbucks' or 'Race Together' into positive, negative, or neutral class using the random forest algorithm. Figures 19, 20, and 21 below show the total number of negative, neutral, positive and tweets per hour for the time period between 3/22/2015 and 3/28/2015 respectively. Figure 22 shows the total number of each category: positive, neutral and negative tweets per day for the same time period. As shown in Figure 22, there was no remarkable change in the number of each polarity category. Considering that the collected tweets were posted a week after the 'Race Together' campaign started on 3/16/2015, this may indicate that there were no significant emotional effects.

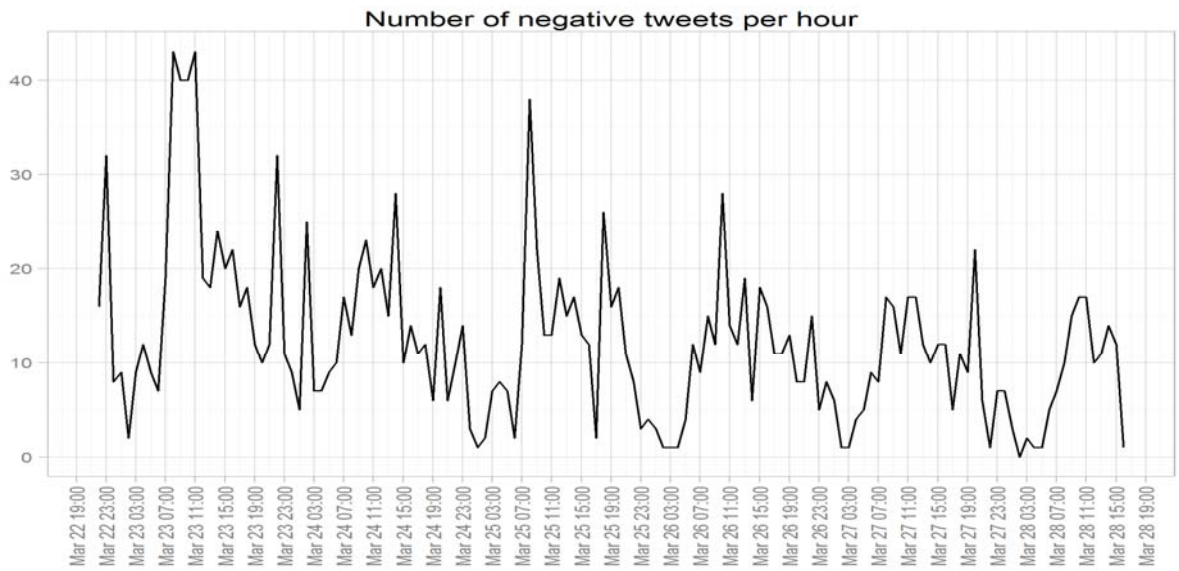

Figure 19 Number of negative tweets per hour for the time period between 3/22/2015 – 3/28/2015 (Starbucks)

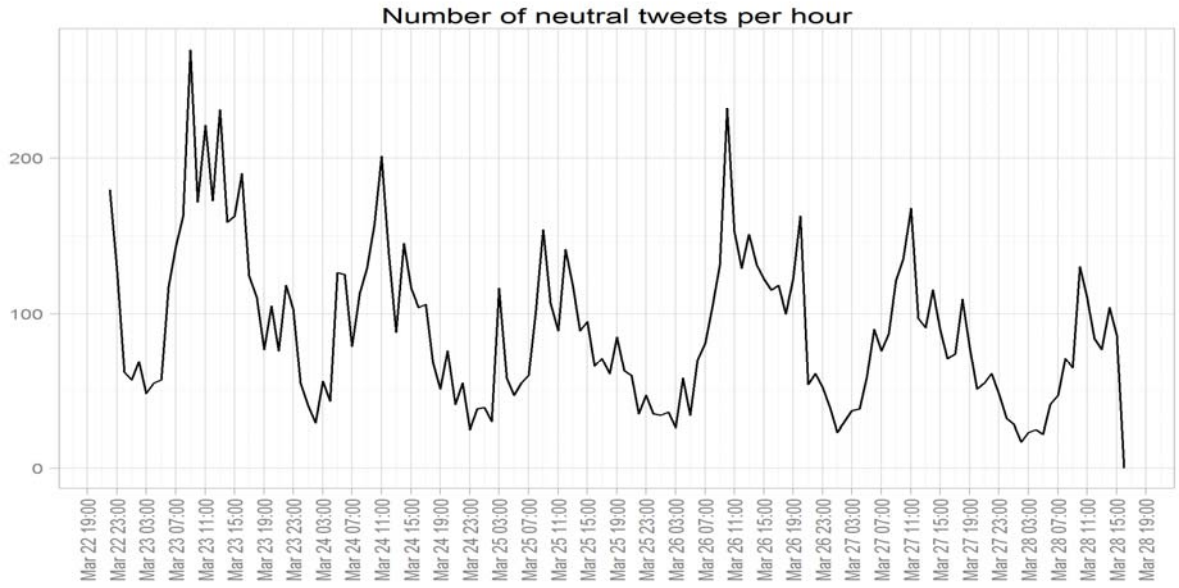

Figure 20 Number of neutral tweets per hour for the time period between 3/22/2015 – 3/28/2015 (Starbucks)

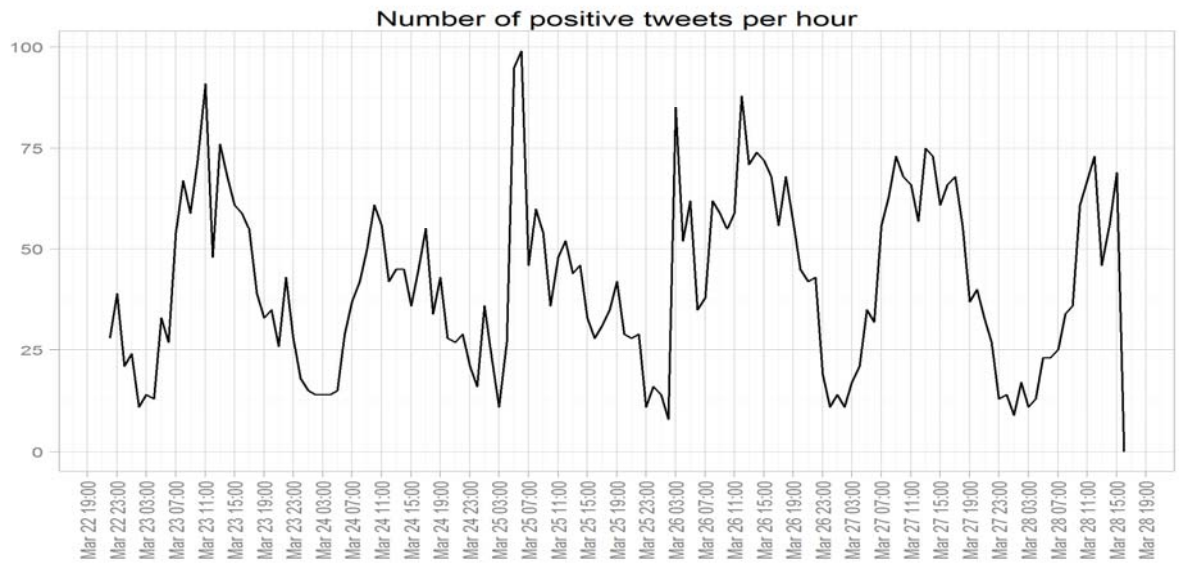

Figure 21 Number of positive tweets per hour for the time period between 3/22/2015 – 3/28/2015 (Starbucks)

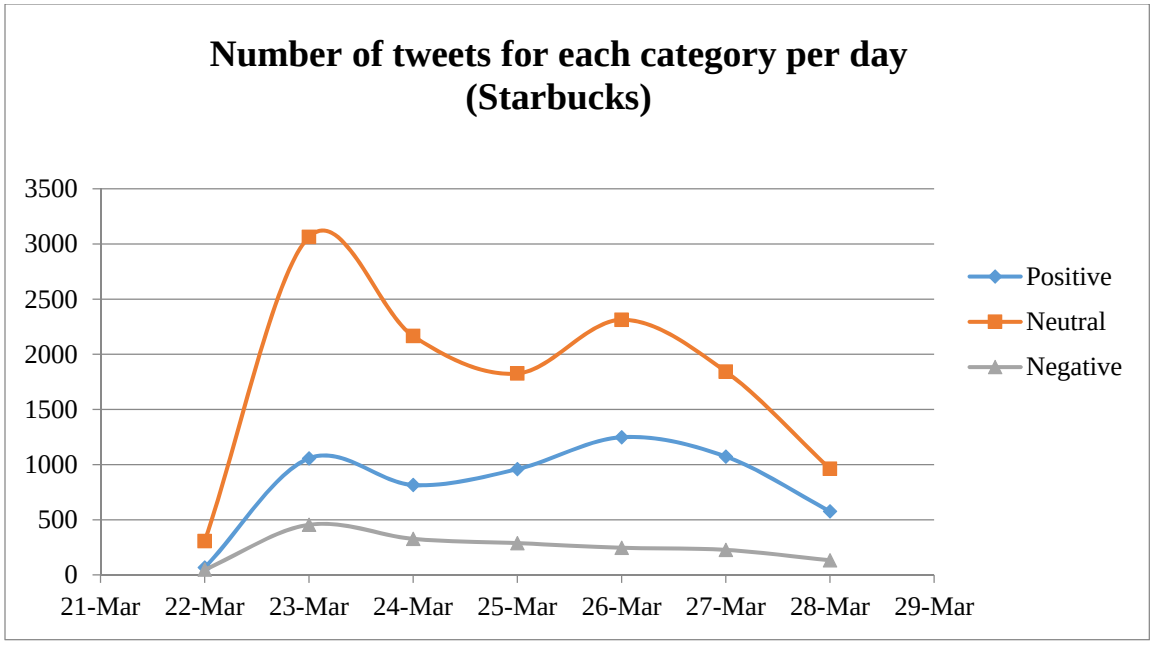

Figure 22 Total numbers of tweets of each category per day for the time period between 3/22/2015 – 3/28/2015 (Starbucks)

Except for the neutral tweets on 3/23, the total numbers of the tweets posted during the sample time period does not show any remarkable changes (Figure 23). The high number

of neutral tweets on 3/23 may be affected by the fact that Starbucks announced that they would cease the Race Together campaign on that day and news media outlets posted such news on Twitter. Overall, the lack of significant changes in the total number of tweets may suggest that this once high profile campaign is no longer interesting to many users, thus it is not a significant reputational risk factor that could damage the company's reputation.

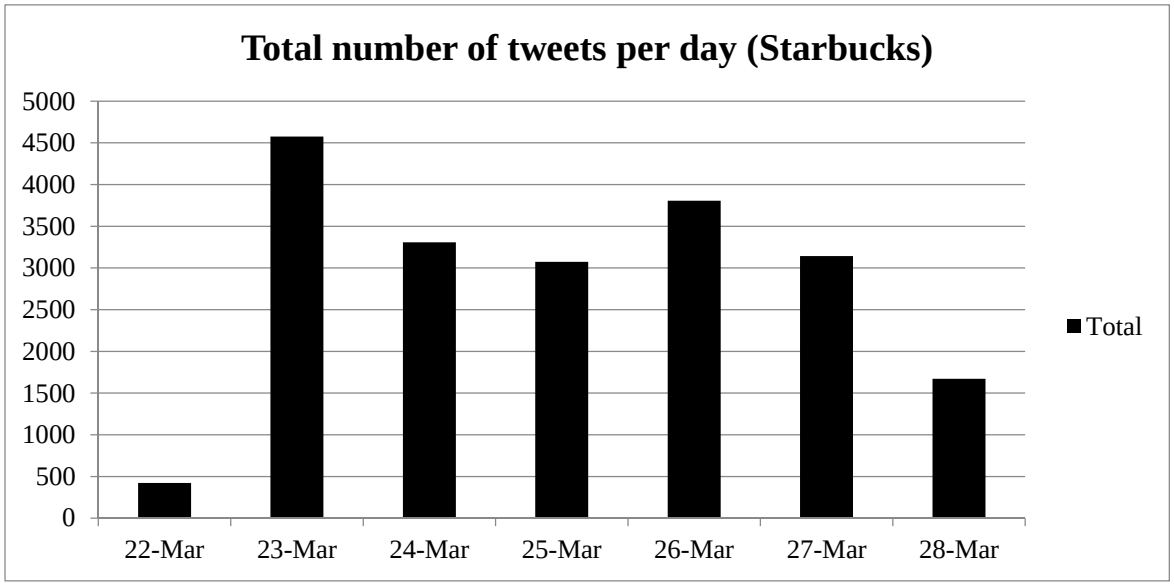

Figure 23 Total number of tweets per each day for the time period between 3/22/2015 – 3/28/2015 (Starbucks)

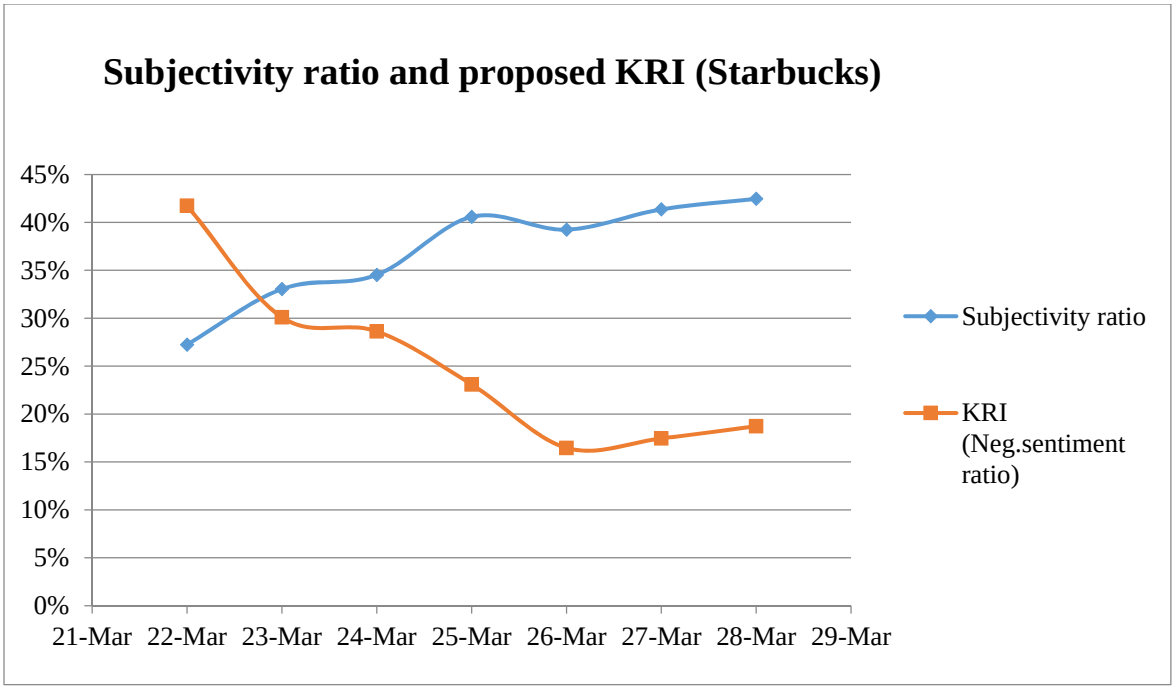

Figure 24 Ratio of subjective tweets to total number of tweets vs. the ratio of negative tweets to the total subjective tweets (Starbucks)

The KRI measured on the collected tweets confirms this interpretation. As shown in Figure 24, the values of the proposed KRI over the sample time period show that the users' negative tweet messages were decreasing as the time passed, while positive tweets messages were steadily increasing. This may indicate that 'Race Together' is not likely to result in significant reputational damage to Starbucks. This information would help the risk based auditor to evaluate the potential adverse effect of a given event on Starbucks' reputation.

Given the abundant sources of comments on the internet, the auditor may measure and monitor such KRIs that represent the people's negative emotions in real time. Along with other relevant KRIs, a KRI extracting negative perception from real time social media may help the risk based auditor to assess the company's current reputation in real time,

thus timely detecting when the company's reputation gets damaged significantly and take mitigating action.

4.6 Conclusion and Limitations

The objective of this chapter is to demonstrate how relevant KRIs can be designed and measured to assess and monitor reputation risk in real time under the proposed CRMA methodology. As an example of such KRIs that could measure the current status of the organization's reputation, we propose a KRI that would represent negative perception about a company using real time social media data. To further demonstrate the proposed KRI, we use two real reputational risk events. We perform the sentiment analysis to measure the proposed KRI and observe that it indeed catches changes in people's negative perceptions about the given events. In general, the proposed KRI would be able to track in a real time manner how people perceive a given reputational risk event through their subjective thoughts posted on Internet based real time social media platforms. The risk based auditor would benefit utilizing such abundantly available real time social media data to extract their stakeholders' perceptions of the organization and assess and monitor the organization's reputation in a more continuous and real time manner.

However, there are a number of limitations in our sentiment analysis. First, the Twitter data we collected for the analysis covers only 5 to 6 days which could be too short a period to fully understand and infer true trends of users' negative sentiments embedded in their tweets regarding the given reputational risk event. Since Twitter provides limited historical data, the maximum time we could go back was only 5 to 6 days. If we had relevant tweets posted over a longer period of time, the results may have been different.

Second, the performance of our sentiment classification analysis may be limited due to domain dependency (Pang and Lee, 2008). We trained our classifiers on test data used by Thelwall et al. (2012) to demonstrate their SentiStrengh 2 algorithm. Although these data sets include informal and short texts similar to our sampled tweet messages, their domains do not necessarily correspond to ours. Therefore, using classifiers trained on such different domain subject data sets in each of our reputational risk event examples may result in poor performance on classification on our sampled tweet text for each reputational risk events. If we had training data sets with a similar domain, results may differ.

Third, our classification results could change as we use other algorithms. That is, depending on which algorithm we use to classify the tweet corpus, results may differ. We attempted 3 classification machine learning algorithms: naïve Bayes, SVM, and random forest. Among these algorithms, we chose random forest as our main classifier algorithm because it gives the highest accuracy rate across all classifier categories, particularly negative tweets (*Table 12*). However, by finding optimal parameters and using them along with more domain specific training data sets, other classification algorithms may perform better, resulting in different outcomes.

Chapter 5: Summary, Contributions, Limitations and Future research

5.1 Summary

In this dissertation, we describe the key concepts and background of CRMA and propose a methodology for its development. Drawing on the original suggestion in Vasarhelyi et al., 2010, the proposed development methodology provides procedures to build a continuous risk assessment and dynamic audit planning process for a risk based audit. We define CRMA as a type of CA procedure that enables continuous risk assessments and dynamic audit planning to monitor and assess changes to risk exposure levels in real time, prioritizing subsequent audit and risk management procedures according to these changes.

First, we discuss the background of the BRA method, practice, and related auditing standards. BRA has been widely implemented since the 1990s, but there is a lack of guidance on the risk assessment and linking processes that are critical for an effective BRA implementation (Bell et al., 1997; Knechel, 2007; Robson et al., 2007). The proposed CRMA methodology provides guidance on how an auditor should monitor and assess the client's constantly changing business risks and link them to subsequent audit risk analysis and relevant audit procedure.

The proposed methodology utilizes Key Risk Indicators (KRIs, Institute of Operational Risk, 2010) to monitor risk exposure in real time. As a CA procedure, CRMA takes advantage of the organization's integrated and automated information system to access and analyze the organization's internal and external data sources to compute and monitor relevant KRIs in a close to the event manner.

We argue that a risk based auditor should not just focus on what events would occur in future, but also the risks events that have already occurred and affected the organization's

business processes and related audit risks. For such purpose, the proposed CRMA methodology uses both leading indicators and CEIs (Confirmatory Event Indicators) to better anticipate the potential risk events to be likely happen (i.e., leading indicators) and understand the status of the risk events that may have occurred already (i.e., confirming what risk events have occurred and whether their adverse impacts are well mitigated).

The proposed CRMA methodology suggests using pre-established links between business risks and audit and risk management procedures, which are configured in advance. Building links beforehand would enable the auditor to identify the audit implications of the organization's business risks.

The most important step in the proposed CRMA methodology is the development and measurement of relevant KRIs in a continuous manner for the rapid monitoring of risks. Big data, digital processes, integrated business information systems, and social media are additional data sources for an auditor to extract and develop relevant KRIs. We present a KRI that represents the public's negative perception of an organization measured from real time social media data, which may help the auditor to evaluate the effect of a risk event on the organization's reputation. We demonstrate the present KRI by using the two real risk events: Purina's lawsuit for selling harmful dog food and Starbucks' 'Race Together' campaign, and the Twitter messages ('tweets') mentioning these events. We perform a sentiment analysis to classify the tweets into positive and negative polarities. We observe that the present KRI indeed catches changes in the degree of the public's negative perception in response to the risk events. For example, there was an increasing number of negative sentiments expressed in tweets discussing Purina's lawsuit, which may indicate that Purina's reputation may have been damaged. For Starbucks' case, the

present KRI caught that there were no significant public response to the event. Furthermore, it revealed that the proportion of negative tweets were rather reduced after the company halted the campaign, suggesting that the event was no longer threats to the company.

5.2 Contributions

The contributions of this dissertation study are threefold. First, the present study contributes to CA research. Vasarhelyi et al. (2010) point out that since an organization's business and audit environment change constantly, and since contemporary audit standards require a risk based approach, today's CA system should be risk driven and dynamic. They suggest developing a CRMA system that continuously monitors and assesses an organization's risks and prioritizes audit and risk management procedures. We refine these concepts and propose an operationalizing methodology for the first time.

Second, a lack of guidance on continuous risk assessment is a major obstacle to implementing an effective BRA process. We develop a CRMA methodology that involves ongoing risk assessment and links the client's business risks to relevant audit and risk management procedures. The proposed methodology suggests a new approach to building a CRMA process and develops a link between client business risk assessments and audit risk assessments for an effective BRA process. As such, the present study on CRMA contributes to the BRA literature.

Third, the present study contributes to the KRI literature. The proposed methodology suggests using relevant KRIs to measure and monitor risk exposure levels in a continuous and real time manner for an effective risk based audit practice. The present study

introduces such a measure for the first time. We further propose a KRI that measures the lagging effect of a risk event on an organization's reputation. The present KRI would help a risk based auditor to assess and monitor changes in a client's reputation in a close to the event manner as it is measured from real time social media data.

5.3 Limitations and Future Research

There are a number of limitations in the present study. First, according to the original framework (Vasarhelyi et al., 2010), CRMA takes advantage of the organization's automated and integrated IT systems and computerized algorithms to continuously monitor and assess the organization's risks and automatically prioritize subsequent audit procedures to minimize audit risk and the organization's risk exposure. The present study reviews this original work on CRMA, its underlying motivations, and its purposes. We propose a methodology for CRMA to assess and monitor the organization's risk exposure levels, how the changes in the organization's risks can be recognized in a real time manner, and how the relevant audit and risk management procedures can be prioritized and re-prioritized automatically whenever changes in the organization's risk profiles occur. We have not designed specific algorithms or prescriptive normalization and weighting methods for these procedures. We leave this for future research.

Second, CRMA is initially proposed as a third procedural component of CA, which interacts with other CA procedures, CDA or CCM. If CDA and/or CCM procedures are continuously adjusted by input from CRMA, they would become risk based CA procedures that focus on high risk areas, shifting CA into a risk responsive dynamic system. Therefore, linking CRMA to CDA or/and CCM would be critical to changing a static CA system to a risk driven system. However, the present study provides no

guidance on that matter as we limit our focus to CRMA. We leave this important research for future study.

Third, in our sentiment analysis to measure the present KRI, the Twitter data we collected for the analysis covers only 5 to 6 days which could be too short a period to fully understand and infer true trends of users' negative sentiments embedded in their tweets regarding the given reputational risk event. If we had relevant tweets posted over a longer time period, the results may have been different.

Fourth, the performance of our sentiment classification analysis may be limited by domain dependency (Pang and Lee, 2008). We trained our classifiers on data sets used by Thelwall et al. (2012) to demonstrate their sentiment classification algorithm (SentiStrengh 2). These data sets include 11,820 short informal texts from 6 different sites. Although these data sets include informal and short texts similar to typical tweets, their domains do not necessarily correspond to our context. Therefore, using classifiers trained on different domains to classify our test data may result in different classification.

Fifth, our classification results could change with the use of other classification algorithms. We attempted 3 classification machine learning algorithms: naïve Bayes, SVM, and random forest. Among these algorithms, we chose random forest because it gives the highest average accuracy across all classifier categories. However, by finding optimal parameters and using more domain specific training data sets, other classification algorithms may perform better than random forest.

Sixth, another important future research agenda is to further examine the usefulness of the proposed KRI as a metric to measure an organization's reputation by validating it

with the organization's market or financial performance data. The proposed KRI is able to track the public's negative perception of an organization in close to real time as it is measured from real time social media data. We show that the present KRI indeed captures the changes in the public's negative sentiments in response to certain risk event of an organization and suggests that it could provide a real time signal for an organization's reputation damage. We argue that continuous monitoring such a KRI may help risk based auditors to timely detect the organization's unanticipated reputational damage and take prompt actions to address its related audit implications and mitigate the further damage.

However, whether the present KRI truly represents an organization's ongoing reputation damage may be empirically tested with the organization's associated market and/or financial performance data which are to be affected by the damaged reputation. For example, researchers may examine whether an increasing trend in the public's negative perception of an organization measured by the present KRI is correlated with the changes in the organization's stock quotes or sales amounts over the same time period when such increasing trend is observed. A correlation between the public's negative perceptions of the organization measured from the present KRI and their poor financial or market performance data may suggest that the present KRI indeed represents the organization's current reputation damage.

The most extant studies use Fortune's AMAC reputation scores as a proxy to measure an organization's reputation level, which heavily weight organizations' prior financial performance in computing their reputation scores (Ponzi et al., 2011; Fryxell and Wang, 1994; Brown and Perry, 1994). The present KRI may be used as an alternate proxy to

measure an organization's reputation level, which better reflects changes in the stakeholders' emotional perception of the organization in close to *real time* manner. We believe that research on this area would also contribute to the corporate reputation literature.

References

Abbott, A. (1988). The system of professions: an essay on the division of expert labour. Chicago: University of Chicago Press.

Abbasi, A., Hassan, A., & Dhar, M. (2014). Benchmarking Twitter Sentiment Analysis Tools. In Proceedings of the Ninth International Conference on Language Resources and Evaluation (LREC'14) (pp. 823-829).

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

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

Alles, M.G., Kogan, A., and Vasarhelyi (2008). Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementations, Journal of Information Systems, 22(2), 195-214.

Allen, R. D., Hermanson, D. R., Kozloski, T. M., & Ramsay, R. J. (2006). Auditor risk assessment: Insights from the academic literature. Accounting Horizons, 20(2), 157-177.

Allegrini, M., & D'Onza, G. (2003). Internal auditing and risk assessment in large Italian companies: an empirical survey. International Journal of Auditing, 7(3), 191-208.

American Institute of Certified Public Accountants. (2002). Consideration of Fraud in a Financial Statement Audit. Statement on Auditing Standards No.99. New York, NY: AICPA.

_____. (2006a). Audit Risk and Materiality in Conducting an Audit. Statement on Auditing Standards No. 107. New York, NY: AICPA.

_____. (2006b). Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement. Statement on Auditing Standards No. 109. New York, NY: AICPA.

_____. (2006c). Statements on Auditing Standards Nos. 104-111. New York, NY: AICPA. Available at <http://www.aicpa.org/interestareas/employeebenefitplanauditquality/resources/accountingandauditingresourcecenters/pages/riskassessmentstandards(sasnos104-111).aspx>

Asur, S., & Huberman, B. (2010, August). Predicting the future with social media. In Web Intelligence and Intelligent Agent Technology (WI-IAT), 2010 IEEE/WIC/ACM International Conference on (Vol. 1, pp. 492-499). IEEE.

Aven, T. (2013). On the meaning of a black swan in a risk context. Safety science, 57, 44-51.

Bagshaw, K. (1999). The key to a good audit. Accountancy, 124, 96.

Ballou, B., & Knechel, W. R. (2002). Ceskoslovenská Obchodní Banka, as: applying business risk audit techniques in an emerging market economy. Issues in Accounting Education, 17(3), 289-313.

Ballou, B., Earley, C. E., & Rich, J. S. (2004). The impact of strategic-positioning information on auditor judgments about business-process performance. Auditing: A Journal of Practice & Theory, 23(2), 71-88.

Bandura, R. (2008). A survey of composite indices measuring country performance: 2008 update. Office of Development Studies, New York: United Nations Development Programme.

Barger, L. K., Cade, B. E., Ayas, N. T., Cronin, J. W., Rosner, B., Speizer, F. E., & Czeisler, C. A. (2005). Extended work shifts and the risk of motor vehicle crashes among interns. New England Journal of Medicine, 352(2), 125-134.

Barnett, M. L., Jermier, J. M., & Lafferty, B. A. (2006). Corporate reputation: The definitional landscape. Corporate reputation review, 9(1), 26-38.

Basel Committee on Banking Supervision. (2008). Liquidity risk: Management and supervisory challenges. Basel, BIS. < http://www.bis.org/publ/bcbs136.pdf>

Basel Committee Banking Supervision. (2008). Principles for sound liquidity risk management and supervision. Basel, BIS < http://www.bis.org/publ/bcbs144.pdf>

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2010). How key risk indicators can sharpen focus on emerging risks. Mark L. Frigo and Richard J. Anderson (COSO-Jan 2011): Practical Approaches for Getting Started.

Bell, T.B., Marrs, F.O., Solomon, I, and Thomas, H. (1997). Auditing organizations through a strategic-systems lens: The KPMG business measurement process. KPMG LLP

Bell, T. B, Peecher, M. E. & Solomon, I. (2002). Cases in strategic-systems auditing: KPMG and University of Illinois at Urbana-Champaign Business Measurement Case Development and Research Program, KPMG LLP.

_____. (2005). The 21st Century Public Company Audit, Conceptual Elements of KPMG's Global Audit Methodology

Bergh, D. D., Ketchen, D. J., Boyd, B. K., & Bergh, J. (2010). New frontiers of the reputation—Performance relationship: Insights from multiple theories. Journal of Management, 36(3), 620-632.

Bierstaker, J. L., & Wright, A. (2004). Does the adoption of a business risk audit approach change internal control documentation and testing practices?. International Journal of Auditing, 8(1), 67-78.

Bifet, A., & Frank, E. (2010, January). Sentiment knowledge discovery in twitter streaming data. In Discovery Science (pp. 1-15). Springer Berlin Heidelberg.

Black, E. L., Carnes, T. A., & Richardson, V. J. (2000). The market valuation of corporate reputation. Corporate Reputation Review, 3(1), 31-42.

Blokdijk, H., Drieenhuizen, F., Simunic, D. A., & Stein, M. T. (2003). Determinants of the mix of audit procedures: Key factors that cause auditors to change what they do. Sauder School of Business, The University of British Columbia, Forthcoming.

Boehm, B. W., & Ross, R. (1989). Theory-W software project management principles and examples. Software Engineering, IEEE Transactions on, 15(7), 902-916.

Bollen, J., Pepe, A., & Mao, H. (2009). Modeling public mood and emotion: Twitter sentiment and socio-economic phenomena. arXiv preprint arXiv:0911.1583.

Bou-Raad, G. (2000). Internal auditors and a value-added approach: the new business regime. Managerial Auditing Journal, 15(4), 182-187.

Boyd, B. K., Bergh, D. D., & Ketchen, D. J. (2010). Reconsidering the reputation—performance relationship: A resource-based view. Journal of Management, 36(3), 588-609.

Boyd, D., Golder, S., & Lotan, G. (2010, January). Tweet, tweet, retweet: Conversational aspects of retweeting on twitter. In System Sciences (HICSS), 2010 43rd Hawaii International Conference on (pp. 1-10). IEEE.

Bovee, M., Kogan, A., Nelson, K., Srivastava, R. P., & Vasarhelyi, M. A. (2005). Financial reporting and auditing agent with net knowledge (FRAANK) and extensible business reporting language (XBRL). Journal of Information Systems, 19(1), 19-41.

Bravo-Marquez, F., Mendoza, M., & Poblete, B. (2013, August). Combining strengths, emotions and polarities for boosting Twitter sentiment analysis. In Proceedings of the Second International Workshop on Issues of Sentiment Discovery and Opinion Mining (p. 2). ACM.

Bremmer, I., (2005), Managing Risk in an Unstable World, Harvard Business Review, June 2005

Brown, B., & Perry, S. (1994). Removing the financial performance halo from Fortune's "Most Admired" companies. Academy of Management Journal, 37(5), 1347-1359.

Brown, C.E., Wong, J.A., and Baldwin, A.A. (2007), A Review and Analysis of the Existing Research Streams in Continuous Auditing, Journal of Emerging Technologies in Accounting: 4(1), 1-28.

Bumgarner, N and Vasarhelyi, M. (2014). Continuous Auditing: A New View, Pink Book, Chapter 1.

Burnaby, P. A., & Hass, S. (2011). Internal auditing in the Americas. Managerial Auditing Journal, 26(8), 734-756.

Cabral, L., & Hortacsu, A. (2004). The dynamics of seller reputation: Theory and evidence from eBay (No. w10363). National Bureau of Economic Research.

Cao, Y., Myers, L. A., & Omer, T. C. (2012). Does Company Reputation Matter for Financial Reporting Quality? Evidence from Restatements*. Contemporary Accounting Research, 29(3), 956-990.

Cao, Y., Myers, J. N., Myers, L. A., & Omer, T. C. (2015). Company reputation and the cost of equity capital. Review of Accounting Studies, 20(1), 42-81.

Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants (CICA/AICPA). (1999). Continuous Auditing. Research report. Toronto, Canada: CICA.

Casado, A. M., Peláez, J. I., & Cardona, J. (2014). Managing corporate reputation: A perspective on the Spanish market. Corporate Reputation Review, 17(1), 46-63.

Carnaghan, C. (2006). Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison. International Journal of Accounting Information Systems, 7(2), 170-204.

Carcello, J. V., Hermanson, D. R., & Raghunandan, K. (2005). Factors associated with US public companies' investment in internal auditing. Accounting Horizons, 19(2), 69-84.

Chan. D.Y. and Vasarhelyi. M.V. (2011), Innovation and practice of continuous auditing, International Journal of Accounting Information Systems, 12, 152-160.

Chiu, V., Liu, Q., and Vasarhelyi, M.A. (2013), The Development and Intellectual Structure of Continuous Auditing Research, Journal of Accounting Literature, Forthcoming.

Chow, C. C., & Sarin, R. K. (2002). Known, unknown, and unknowable uncertainties. Theory and Decision, *52*(2), 127-138.

Chun, R. (2005). Ethical character and virtue of organizations: An empirical assessment and strategic implications. Journal of Business Ethics, 57(3), 269-284.

Colbert, J. L., & Wayne Alderman, C. (1995). A risk-driven approach to the internal audit. Managerial Auditing Journal, 10(2), 38-44.

Committee of Sponsoring Organizations of the Treadway Commission. (1992). Internal Control – Integrated Framework. COSO.

_____. (2004). Enterprise risk management - Integrated Framework. COSO.

_____. (2013). Internal Control— Integrated Framework, Executive Summary. *(Updated version of 1992's Internal Control framework)* <http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf>

CNN (2015). Lawsuit says Purina food harms dogs; company denies allegations. February, 2015. Available at < http://www.cnn.com/2015/02/24/us/dog-food-lawsuit/>

Curtis, E., & Turley, S. (2007). The business risk audit–A longitudinal case study of an audit engagement. Accounting, Organizations and Society, 32(4), 439-461.

Cushing, B.E. and Loebbecke, J.K. (1983), Analytical Approaches to Audit Risk: Survey and Analysis, Auditing: A Journal of Practice and Theory, 3, 23-41.

Das, S. R., & Chen, M. Y. (2007). Yahoo! for Amazon: Sentiment extraction from small talk on the web. Management Science, 53(9), 1375-1388.

Davenport, T. H., & Dyché, J. (2013). Big data in big companies. May 2013.

Davies, J., Finlay, M., McLenaghen, T., & Wilson, D. (2006). Key risk indicators–their role in operational risk management and measurement. ARM and RiskBusiness International, Prague, 1-32.

Dean, J. (2014). Big Data, Data Mining, and Machine Learning: Value Creation for Business Leaders and Practitioners. John Wiley & Sons.

Debreceny, R., Gray, G. L., Tham, W. L., Goh, K. Y., & Tang, P. L. (2003). The development of embedded audit modules to support continuous monitoring in the electronic commerce environment. International Journal of Auditing, 7(2), 169-185.

Debreceny, R.S., Gray, G.L., Ng, J.J., Lee, K.S., and Yau, W.F. (2005), Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Functionality, Journal of Information Systems, 19(2), 7-27.

Diakopoulos, N. A., & Shamma, D. A. (2010, April). Characterizing debate performance via aggregated twitter sentiment. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1195-1198). ACM.

Dimitriadou, E., Hornik, K., Leisch, F., Meyer, D., & Weingessel, A. (2005). e1071: Misc Functions of the Department of Statistics (e1071), TU Wien, Version 1.5-11. URL http://CRAN. R-project. org.

Dixon, M. R., & Schreiber, J. E. (2011). Near-miss effects on response latencies and win estimations of slot machine players. The Psychological Record, 54(3), 1.

Dowling, G. (2006). Reputation risk: it is the board's ultimate responsibility. Journal of Business Strategy, 27(2), 59-68.

DuVander, A. (2012). 5,000 APIs: Facebook, Google and Twitter Are Changing the Web. ProgrammableWeb. Retrieved August 9, 2012.

Eccles, R. G., Newquist, S. C., & Schatz, R. (2007). Reputation and its risks. Harvard Business Review, 85(2), 104-14.

Eilifsen, A, W. Knechel, R, & Wallage, P. (2001), Application of the Business Risk Audit Model: A Field Study, 15, 193-207

Elliot, R.K. (2002). Twenty-First Century Assurance, Auditing: A Journal of Practice & Theory, 21(1).

Ernst & Young (2013). Key Considerations for your internal audit plan. EYGM Limited. May, 2013. < http://www.ey.com/Publication/vwLUAssets/EY_Key_considerations_for_your_internal_audit_plan_1/$FILE/ATT5QP7A.pdf>

Federal Deposit Insurance Corporation (2004). Off Balance Sheet Activity. FDIC. <https://www.fdic.gov/regulations/safety/manual/section3-8.pdf>

Feinerer, I., Hornik, K., & Feinerer, M. I. (2015). Package ‘tm’. Corpus, 10, 1.

Finlay, M. (2004). A Structured Framework for KRIs,". OpRisk&Compliance”, July.

Flanagan, D. J., & O’Shaughnessy, K. C. (2005). The effect of layoffs on firm reputation. Journal of management, 31(3), 445-463.

Fombrun, C. (1996). Reputation. John Wiley & Sons, Ltd.

Fombrun, C., & Van Riel, C. (1997). The reputational landscape. Corporate reputation review, 1-16.

Fombrun, C. J., Gardberg, N. A., & Sever, J. M. (2000). The reputation quotient: A multi-stakeholder measure of corporate reputation. Journal of Brand Management.

Fombrun, C. J. (2007). List of lists: A compilation of international corporate reputation ratings. Corporate Reputation Review, 10(2), 144-153.

Friedman, B. A. (2009). Human resource management role implications for corporate reputation. Corporate Reputation Review, 12(3), 229-244.

Freudenberg, M. (2003). Composite Indicators of Country Performance, OECD

Fryxell, G. E., & Wang, J. (1994). The fortune corporate'reputation'index: Reputation for what?. Journal of management, 20(1), 1-14.

Gilbert, E., & Karahalios, K. (2010, May). Widespread Worry and the Stock Market. In ICWSM (pp. 59-65).

Go, A., Huang, L., & Bhayani, R. (2009). Twitter sentiment analysis. Entropy, 17.

Gramling, A. A., CIA, C., Ramamoorti, S., CIA, A., & CFSA, C. (2003). Research Opportunities in Internal Auditing, Chapter 1, Institute of Internal Auditors Research Foundation.

Grabowski, M., Ayyalasomayajula, P., Merric, J., Harrald, J.R., and Roberts, K. (2007). Leading indicators of safety in virtual organization. Safety Science, 45, 1013-1043

Groomer, S.M. and Murthy, U.S. (1989). Continuous Auditing of Database Applications: An Embedded Audit Module Approach, Spring.

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

Helm, S. (2005). Designing a formative measure for corporate reputation. Corporate reputation review, 8(2), 95-109.

Herring, S. C., & Honeycutt, C. (2009). Beyond microblogging: Conversation and collaboration via Twitter. Extraído el, 10.

Highhouse, S., Broadfoot, A., Yugo, J. E., & Devendorf, S. A. (2009). Examining corporate reputation judgments with generalizability theory. Journal of Applied Psychology, 94(3), 782.

Hoffman, T. (2008). Online reputation management is hot—but is it ethical. Computerworld, February.

Honey, C., & Herring, S. C. (2009, January). Beyond microblogging: Conversation and collaboration via Twitter. In System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on (pp. 1-10). IEEE.

Houston, R. W. Peters, M.F. & Pratt. J.H. (1999) The Audit Risk Model, Business Risk and Audit-Planning Decisions, The Accounting Review, 74, July, 281-298

Hughes, A. L., & Palen, L. (2009). Twitter adoption and use in mass convergence and emergency events. International Journal of Emergency Management, 6(3-4), 248-260.

Hwang, S. (2010), Identifying and Communicating Key Risk Indicators, Enterprise Risk Management, John Wiley & Sons, Inc., Hoboken, NJ

Imhoff, G. (2003). Accounting quality, auditing and corporate governance. Auditing and Corporate Governance (January 2003).

International Auditing and Assurance Standards Board (IAASB). (2014). International Standard on Auditing No. 315. Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements 2014 Edition

IIA (The Institute of Internal Auditors). (2009). Position Paper: The Role of Internal Auditing in Enterprise-eide Risk Management. The Institute of Internal Auditors. Altamonte Springs, FL.

_____. (2010). Practice Advisories under Professional Practice Framework. The Institute of Internal Auditors, Altamonte Springs, FL.

_____. (2012). International standards for the professional practice of internal auditing. The Institute of Internal Auditors, Altamonte Springs, FL.

Institute of Operational Risk. (2010). Operational Risk Sound Practice Guidance: Key Risk Indicators, November 2010, The Institute of Operational Risk.

ISO 31000 (2009). Risk management – Principles and guidelines, ISO, 2009

Jackson, A. B., Moldrich, M., & Roebuck, P. (2008). Mandatory audit firm rotation and audit quality. Managerial Auditing Journal, 23(5), 420-437.

Jared, D., (2014) Big Data, Data Mining, and Machine Learning, Wiley and SAS Business Series, Hoboken, NJ

Janvrin, D. J., Payne, E. A., Byrnes, P., Schneider, G. P., & Curtis, M. B. (2012). The updated COSO Internal Control-Integrated Framework: Recommendations and opportunities for future research. Journal of Information Systems, 26(2), 189-213.

Jeppesen, K. K. (1998). Reinventing auditing, redefining consulting and independence. European Accounting Review, 7(3), 517-539.

Kaplan, S. (1990). On the inclusion of precursor and near miss events in quantitative risk assessments: A Bayesian point of view and a space shuttle example. Reliability Engineering & System Safety, 27(1), 103-115.

Kim, S. M., & Hovy, E. (2006). Automatic identification of pro and con reasons in online reviews. In Proceedings of the COLING/ACL on Main conference poster sessions (pp. 483-490). Association for Computational Linguistics.

Kinney, W. R. (1997), Foreword to Auditing Organizations through a Strategic-Systems Lens – the KPMG Business Measurement Process, Bell, T., Marrs, F., Solomon, I. and Thomas, H. 1997, KPMG, Montvale NJ.

Kinney Jr, W. R. (2005). Twenty-five years of audit deregulation and re-regulation: What does it mean for 2005 and beyond?. Auditing: A Journal of Practice & Theory, 24(s-1), 89-109.

Kogan, A., Sudit, E. F., & Vasarhelyi, M. A. (1999). Continuous online auditing: A program of research. Journal of Information Systems, 13(2), 87-103.

Kogan, A., Vasarhelyi, M. A., & Wu, J. (2007). Continuous data level auditing using continuity equations. Working paper, Rutgers Business School, 42(7), 436-452.

Knechel, R.W. (2007), The business risk audit: Origins, obstacles and opportunities, Accounting, Organizations and Society, 32, 383–408

Knechel, W. R., Salterio, S. E., & Kochetova-Kozloski, N. (2010). The effect of benchmarked performance measures and strategic analysis on auditors' risk assessments and mental models. Accounting, Organizations and Society, 35(3), 316-333.

KPMG (2012). Continuous Auditing and Continuous Monitoring: The current status and the road ahead, KPMG's EMA region survey.

_____ (2013). COSO Internal Control – Integrated Framework (2013). KPMG LLP. CA.

Kuhn Jr, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. Journal of Information Systems, 24(1), 91-112.

Kwak, H., Lee, C., Park, H., & Moon, S. (2010, April). What is Twitter, a social network or a news media?. In Proceedings of the 19th international conference on World wide web (pp. 591-600). ACM.

Larkin, J. (2002). Strategic reputation risk management. Palgrave Macmillan.

Lemon, W. M., Tatum, K. W., & Turley, W. S. (2000). Developments in the audit methodologies of large accounting firms. London, UK: ABG Professional Information.

Louwers, T.J., Ramsay, R.J., Sinason, D.h., and Strawser, J.R. (2008). Auditing & Assurance services. New York, NY: McGraw-Hill.

Liu, B., & Zhang, L. (2012). A survey of opinion mining and sentiment analysis. In Mining text data (pp. 415-463). Springer US.

Matz, L. (2008). RISK MEASUREMENT-Defining and Using Liquidity KRIs-Insufficient liquidity can kill the bank suddenly but too much will kill it slowly. Bank Accounting & Finance, 21(5), 39.

McConnell Jr, D. K., & Schweiger, C. H. (2007). Implementing the new ASB risk assessment audit standards. The CPA Journal, 77(6), 20.

McLenaghen, T. (2008). The" Best" Retail Lending KRIs: An Industry Working-Group Perspective-RMA's KRI Retail Banking Working Group has identified its" 18 best KRIs for retail lending" after months of teleconferencing and brainstorming. RMA Journal, 90(5), 46.

Manyika, J., Chui, M, Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., and Byers, A.H., (2011), Big data: The next frontier for innovation, competition, and productivity, Mckinsey Global Institute,

<http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation>

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data. The management revolution. Harvard Bus Rev, 90(10), 61-67.

Miller, K. D. (1992). A framework for integrated risk management in international business. Journal of international business studies, 311-331.

Moeller, R. R. (2009). Brink's modern internal auditing: A common body of knowledge. John Wiley & Sons.

Moosa, I. (2007). Operational risk management. Palgrave-Macmillan.

Nahl, D., & Bilal, D. (2007). Information and emotion: The emergent affective paradigm in information behavior research and theory. Information Today, Inc.

Nardo, M., Saisana, M., Saltelli, A., Tarantola, S., Hoffman, A., & Giovannini, E. (2005). Handbook on constructing composite indicators, OECD

Nafday, A. M. (2011). Consequence-based structural design approach for black swan events. Structural Safety, 33(1), 108-114.

New York Stock Exchange (2004), Corporate Governance Rules – Section 303A, New York Stock Exchange, New York, NJ, p.14.

O'Connor, B., Krieger, M., & Ahn, D. (2010, May). TweetMotif: Exploratory Search and Topic Summarization for Twitter. In ICWSM.

O'Donnell, E., & Schultz Jr, J. J. (2003). The influence of business-process-focused audit support software on analytical procedures judgments. Auditing: A Journal of Practice & Theory, 22(2), 265-279.

_____ (2005). The halo effect in business risk audits: Can strategic risk assessment bias auditor judgment about accounting details?. The Accounting Review, 80(3), 921-939.

Øien, K., Utne, I. B., & Herrera, I. A. (2011). Building safety indicators: Part 1–theoretical foundation. Safety science, 49(2), 148-161.

Owsley, S., Sood, S., & Hammond, K. J. (2006). Domain Specific Affective Classification of Documents. In AAAI Spring Symposium: Computational Approaches to Analyzing Weblogs (pp. 181-183).

Pang, B., & Lee, L. (2005, June). Seeing stars: Exploiting class relationships for sentiment categorization with respect to rating scales. In Proceedings of the 43rd Annual Meeting on Association for Computational Linguistics (pp. 115-124). Association for Computational Linguistics.

Pang, B., & Lee, L. (2008). Opinion mining and sentiment analysis. Foundations and trends in information retrieval, 2(1-2), 1-135.

Pariyani, A., Seider, W. D., Oktem, U. G., & Soroush, M. (2011). Dynamic risk analysis using alarm databases to improve process safety and product quality: Part I—Data compaction. AIChE Journal, 58(3), 812-825.

Paté-Cornell, E. (2012). On "Black Swans" and "Perfect Storms": risk analysis and management when statistics are not enough. Risk analysis, 32(11), 1823-1833.

Peecher, M. E., Schwartz, R., & Solomon, I. (2007). It's all about audit quality: Perspectives on strategic-systems auditing. Accounting, Organizations and Society, 32(4), 463-485.

Phimister, J. R., Oktem, U., Kleindorfer, P. R., & Kunreuther, H. (2003). Near-miss incident management in the chemical process industry. Risk Analysis, 23(3), 445-459.

Ponzi, L. J., Fombrun, C. J., & Gardberg, N. A. (2011). RepTrak™ pulse: Conceptualizing and validating a short-form measure of corporate reputation. Corporate Reputation Review, 14(1), 15-35.

Power, M. K. (2003). Auditing and the production of legitimacy. Accounting, organizations and society, 28(4), 379-394.

Pritchard, C. L.. (2015). Risk management: concepts and guidance. 5th edition. CRC Press.

Public Company Accounting Oversight Board (PCAOB). (2004). AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING PERFORMED IN CONJUNCTION WITH AN AUDIT OF FINANCIAL STATEMENTS (superseded by AS No.5). PCAOB Release No. 2004-001 March 9, 2004

Public Company Accounting Oversight Board (PCAOB). (2005). Standing Advisory Group (SAG) Meeting: Risk Assessment in Financial Statement Audits. PCAOB. Available at <http://pcaobus.org/News/Events/Documents/02162005_SAGMeeting/Risk_Assessment.pdf>

_____ (2007). Auditing Standard No. 5: AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS AND RELATED INDEPENDENCE RULE AND CONFORMING AMENDMENTS. PACOB. Release No. 2007-005A June 12, 2007

_____ (2010a). AUDITING STANDARDS RELATED TO THE AUDITOR'S ASSESSMENT OF AND RESPONSE TO RISK AND RELATED

AMENDMENTS TO PCAOB STANDARDS. PCAOB Release No. 2010-004 August 5, 2010

_____ (2010b). REPORT ON OBSERVATIONS OF PCAOB INSPECTORS RELATED TO AUDIT RISK AREAS AFFECTED BY THE ECONOMIC CRISIS. PCAOB Release No. 2010-006. September 29, 2010

PwC (2015a), State of the Internal Auditing Profession Study, PwC. <http://www.pwc.com/en_NA/na/assets/pdf/pwc-2015-state-of-the-internal-audit-profession-study.pdf>

____ (2015b). A marketplace without boundaries? PwC 18th Annual Global CEP Survey, <https://www.pwc.com/gx/en/ceo-survey/2015/assets/pwc-18th-annual-global-ceo-survey-jan-2015.pdf>

Ramamoorti, S., Bailey, J., & Traver, R. O. (1999). Risk assessment in internal auditing: a neural network approach. International Journal of Intelligent Systems in Accounting, Finance & Management, 8(3), 159-180.

Ramos, M. (2009). Auditing: Risk-Based Audit Best Practices. Journal of Accountancy, Dec. 2009, 32-37.

Rayner, J. (2004). Managing reputational risk: curbing threats, leveraging opportunities (Vol. 6). John Wiley & Sons.

Read, J. (2005). Using emoticons to reduce dependency in machine learning techniques for sentiment classification. In Proceedings of the ACL student research workshop (pp. 43-48). Association for Computational Linguistics.

Rezaee, Z., Elam, R., & Sharbatoghlie, A. (2001). Continuous auditing: the audit of the future. Managerial Auditing Journal, 16(3), 150-158.

Rezaee, Z. (2010). The importance of internal audit opinions: as their role expands, many auditors are providing opinions on governance, risk management, and internal control. Internal Auditor, 67(2), 47-51.

Risk Management Association (2011), Key Risk Indicators (KRI) Survey, RMA. <http://www.rmahq.org/tools-publications/surveys-studies>

Robert, C. J. (2006). Simple Tools and Techniques for Enterprise Risk Management.

Roberts, P. W., & Dowling, G. R. (2002). Corporate reputation and sustained superior financial performance. Strategic management journal, 23(12), 1077-1093.

Robson, K., Humphrey, C., Khalifa, R. & Jones, J. (2007) Transforming audit technologies: Business risk audit methodologies and the audit field, Accounting, Organizations and Society, 32, 409–438

Ropponen, J., & Lyytinen, K. (2000). Components of software development risk: how to address them? A project manager survey. Software Engineering, IEEE Transactions on, 26(2), 98-112.

Rosenthal, M. M., Cornett, P. L., Sutcliffe, K. M., & Lewton, E. (2005). Beyond the medical record. Journal of general internal medicine, 20(5), 404-409.

Rui, H., Liu, Y., & Whinston, A. (2013). Whose and what chatter matters? The effect of tweets on movie sales. Decision Support Systems, 55(4), 863-870.

Saisana, M., & Tarantola, S. (2002). State-of-the-art report on current methodologies and practices for composite indicator development (p. 214). European Commission, Joint Research Centre, Institute for the Protection and the Security of the Citizen, Technological and Economic Risk Management Unit.

Seki, Y., & Yamazaki, Y. (2006). Effects of working conditions on intravenous medication errors in a Japanese hospital. Journal of nursing management, 14(2), 128-139.

Selim, G., & McNamee, D. (1999). Risk management and internal auditing: what are the essential building blocks for a successful paradigm change. International Journal of Auditing, 3(2), 147-155.

Scandizzo, S. (2005). Risk mapping and key risk indicators in operational risk management. Economic Notes, 34(2), 231-256.

Schneider, G. P., Sheikh, A., & Simione, K. A. (2012). Holistic Risk Management: An Expanded Role for Internal Auditors. Academy of Accounting and Financial Studies Journal, 16(1), 25.

Schultz, J. J., Bierstaker, J. L., & O'Donnell, E. (2010). Integrating business risk into auditor judgment about the risk of material misstatement: The influence of a strategic-systems-audit approach. Accounting, Organizations and Society, 35(2), 238-251.

Schwaiger, M. (2004). Components and parameters of corporate reputation-an empirical study. Schmalenbach business review, 56, 46-71.

Shapiro, C. (1983). Premiums for high quality products as returns to reputations. The quarterly journal of economics, 659-679.

Shi, Z., Rui, H., & Whinston, A. B. (2013). Content sharing in a social broadcasting environment: evidence from twitter. Available at SSRN 2341243.

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. Accounting, Auditing & Accountability Journal, 16(4), 640-661.

Smailovic, J., Kranjc, J., Juršic, M., Grcar, M., Gacnik, M., & Mozetic, I. (2014). Monitoring the Twitter sentiment during the Bulgarian elections.

Stilwell, M.C. and Elliott, R.K. (1985), A Model For Expanding The Attest Function, Journal of Accountancy, 159(5), 66-78

Stulz, R. M. (2008). Risk management failures: What are they and when do they happen?. Journal of Applied Corporate Finance, 20(4), 39-48.

_____. (2009). Six ways companies mismanage risk. Harvard Business Review, 87(

Sundmacher, M., & Ford, G. (2004). Leading Indicators for Operational Risk: Case Studies in Financial Services. Available at SSRN 963235.

Taboada, M., Brooke, J., Tofiloski, M., Voll, K., & Stede, M. (2011). Lexicon-based methods for sentiment analysis. Computational linguistics, 37(2), 267-307.

Taleb, N. N., Goldstein, D. G., & Spitznagel, M. W. (2009). The six mistakes executives make in risk management. Harvard Business Review, 87(10), 78-81.

Taleb, N.N. (2010). The Black Swan: The Impact of the Highly Improbable. 2nd ed. Penguin, London.

Taylor, P., Godino, J. J., & Majeed, B. (2008, June). Use of fuzzy reasoning in the simulation of risk events in business processes. In Proceedings of the 22nd European Conference on Modeling and Simulation (pp. 25-30).

Taylor, C., & Davies, J. (2003). Getting traction with KRIs: laying the groundwork. RMA JOURNAL, 86(3), 58-63.

Taylor, J. B., & Williams, J. C. (2008). A black swan in the money market (No. w13943). National Bureau of Economic Research.

Terpstra, T., de Vries, A., Stronkman, R., & Paradies, G. L. (2012, April). Towards a realtime Twitter analysis during crises for operational crisis management. In Proceedings of the 9th international ISCRAM conference, Vancouver, Canada.

Thelwall, M., Buckley, K., Paltoglou, G., Cai, D., & Kappas, A. (2010). Sentiment strength detection in short informal text. Journal of the American Society for Information Science and Technology, 61(12), 2544-2558.

Thelwall, M., Buckley, K., & Paltoglou, G. (2011). Sentiment in Twitter events. Journal of the American Society for Information Science and Technology, 62(2), 406-418.

Thelwall, M., Buckley, K., & Paltoglou, G. (2012). Sentiment strength detection for the social web. Journal of the American Society for Information Science and Technology, 63(1), 163-173.

The New York Times. (2014). Flight Attendant Kicked Off Korean Air Flight Alleges Cover-Up. December. 2014. Available at

<http://www.nytimes.com/2014/12/19/world/asia/steward-kicked-off-korean-air-flight-accuses-airline-and-south-korea-of-attempting-cover-up.html?_r=1>

Tumasjan, A., Sprenger, T. O., Sandner, P. G., & Welpe, I. M. (2010). Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment. ICWSM, 10, 178-185.

Turney, P. D. (2002). Thumbs up or thumbs down?: semantic orientation applied to unsupervised classification of reviews. In Proceedings of the 40th annual meeting on association for computational linguistics (pp. 417-424). Association for Computational Linguistics.

Vergin, R. C., & Qoronfleh, M. W. (1998). Corporate reputation and the stock market. Business Horizons, 41(1), 19-26.

Vasarhelyi, M. A. and Halper, F.B. (1991). The Continuous Audit of Online Systems, Auditing: A Journal of Practice & Theory, 10(1).

Vasarhelyi, M. A., & Halper, F. B. (2002). Concepts in continuous assurance. Researching accounting as an information systems discipline, 257-271.

Vasarhelyi, M.A., Alles, M.G., Kogan, A. (2004), Principles of Analytic Monitoring for Continuous Assurance, Journal of Emerging Technologies in Accounting, 1, 1-21.

Vasarhelyi, M. A., Alles, M, and Williams K. (2010). Continuous Assurance for the Now Economy, The Institute of Chartered Accountants in Australia.

Waller, W. S. (1993). Auditors' assessments of inherent and control risk in field settings. Accounting Review, 783-803.

Walsh, G., & Beatty, S. E. (2007). Customer-based corporate reputation of a service firm: scale development and validation. Journal of the Academy of Marketing Science, 35(1), 127-143.

Walsh, G., Beatty, S. E., & Shiu, E. M. (2009). The customer-based corporate reputation scale: Replication and short form. Journal of Business Research, 62(10), 924-930.

Warren, J. D., & Parker, X. L. (2003). Continuous auditing: potential for internal auditors. Institute of Internal Auditors Research Foundation.

Wilson, T. D. (2000). Human information behavior. Informing science, 3(2), 49-56.

Wilson, T., Wiebe, J., & Hoffmann, P. (2005, October). Recognizing contextual polarity in phrase-level sentiment analysis. In Proceedings of the conference on human language technology and empirical methods in natural language processing (pp. 347-354). Association for Computational Linguistics.

WSJ (The Wall Street Journal). (2015). Starbucks Ends Key Phase in ‘Race Together’ Campaign. March, 2015. Available at < http://www.wsj.com/articles/starbucks-ends-key-phase-in-race-together-campaign-1427076211>

Wu, W., Zhang, B., & Ostendorf, M. (2010, June). Automatic generation of personalized annotation tags for twitter users. In Human language technologies: The 2010 annual conference of the North American chapter of the association for computational linguistics (pp. 689-692). Association for Computational Linguistics.

de Zwaan, L., Stewart, J., & Subramaniam, N. (2011). Internal audit involvement in enterprise risk management. Managerial auditing journal, 26(7), 586-604.

Zeff, S. A. (2003a). How the US accounting profession got where it is today: Part I. Accounting Horizons, 17(3), 189-205.

Zeff, S. A. (2003b). How the US accounting profession got where it is today: Part II. Accounting Horizons, 17(4), 267-286.