Copyright Warning & Restrictions

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproductions of copyrighted material.

Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be "used for any purpose other than private study, scholarship, or research." If a, user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of "fair use" that user may be liable for copyright infringement,

This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve violation of copyright law.

Please Note: The author retains the copyright while the New Jersey Institute of Technology reserves the right to distribute this thesis or dissertation

Printing note: If you do not wish to print this page, then select "Pages from: first page # to: last page #" on the print dialog screen

NJIT New Jersey's Science & Technology University

The Van Houten library has removed some of the personal information and all signatures from the approval page and biographical sketches of theses and dissertations in order to protect the identity of NJIT graduates and faculty.

ABSTRACT

CONTINUOUS MONITORING OF ENTERPRISE RISKS: A DELPHI FEASIBILITY STUDY

by
Robert Baksa

A constantly evolving regulatory environment, increasing market pressure to improve operations, and rapidly changing business conditions are creating the need for ongoing assurance that organizational risks are continually and adequately mitigated. Enterprises are perpetually exposed to fraud, poor decision making and/or other inefficiencies that can lead to significant financial loss and/or increased levels of operating risk. Increasingly, Information Systems are being harnessed to reinvent the risk management process. One promising technology is Continuous Auditing, which seeks to transform the audit process from periodic reviews of a few transactions to a continuous review of all transactions. However, the highly integrated, rapidly changing and hypercompetitive business environment of many corporations spawns numerous Enterprise Risks that have been excluded from standard risk management processes. An extension of Continuous Auditing is Continuous Monitoring, which is used by management to continually review business processes for unexpected deviations. Using a Delphi, the feasibility and desirability of applying Continuous Monitoring to different Enterprise Risks is studied. This study uncovers a significant relationship between the perceived business value of Continuous Monitoring and years of experience in Risk Management and Auditing, determines that all key architectural components for a Continuous Monitoring system are known, and indicates that Continuous Monitoring may be better suited for monitoring computer crime than monitoring strategic risks such as the loss of a competitive position.

CONTINUOUS MONITORING OF ENTERPRISE RISKS: A DELPHI FEASIBILITY STUDY

By
Robert Baksa

A Dissertation
Submitted to the Faculty of the
New Jersey Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy in Information Systems

Department of Information Systems

May 2015

Copyright © 2015 by Robert Baksa

ALL RIGHTS RESERVED.

APPROVAL PAGE

CONTINUOUS MONITORING OF ENTERPRISE RISKS:
A DELPHI FEASIBILITY STUDY

Robert Baksa

Dr. Murray Turoff, Dissertation Advisor — Date
Distinguished Professor, Emeritus of Information Systems, NJIT

Dr. Roxanne Hiltz, Dissertation Advisor — Date
Distinguished Professor, Emerita of Information Systems, NJIT

Dr. Michael Alles, Committee Member — Date
Associate Professor, School of Business, Rutgers

Dr. Jerry Fjermstad, Committee Member — Date
Professor of Information Systems, NJIT

Dr. Mike Ehlich, Committee Member — Date
Associate Professor of Finance, NJIT

BIOGRAPHICAL SKETCH

Author: Robert Baksa

Degree: Doctor of Philosophy

Date: May 2015

Undergraduate and Graduate Education:

- Doctor of Philosophy in Information Systems,
  New Jersey Institute of Technology, Newark, NJ, 2015

- Master of Business Administration,
  Stern School of Business, New York, NY, 2001

- Master of Science in Information Systems,
  New York University, New York, NY, 1996

- Bachelor of Science in Computer Science and Business,
  University of Pittsburgh, Pittsburgh, PA 1993

Major: Information Systems

Presentations and Publications:

Baksa, R., M. Turoff, et al. (2011). Continuous Auditing as a Foundation for Real Time Decision Support: Implementation Challenges and Successes, *Supporting Real Time Decision-Making: The Role of Context in Decision Support on the Move,* (pp 237-252) New York, NY: Springer.

Baksa, R., M. Turoff, et al. (2010). Continuous Auditing as a Foundation for Real Time Decision Support: Implementation Challenges and Successes. "Proceedings of the 7th International ISCRAM Conference", Seattle, WA, March 2010.

This dissertation is dedicated to my beloved family

To my parents, who have always supported, encouraged and inspired me
To my wife, Sharon, and my daughters, Rachel and Grace,
with whom I have shared the most wonderful moments of my life.

ACKNOWLEDGMENTS

I would like to express my deep and everlasting gratitude to my dissertation advisors, Professors Turoff and Hiltz, for their continued patience, support and guidance throughout this very long endeavor. I would also like to sincerely thank all of my other committee members (i.e., Dr. Michael Alles, Dr. Jerry Fjermestad, and Dr. Mike Ehrlich), whose thoughtful comments have greatly strengthened the overall quality of my dissertation. It has been a great honor to know and work with these incredibly gifted individuals.

I would also like to thank all my clients and colleagues for providing a challenging environment in which to grow and learn; my friends, colleagues and wonderful family, especially my wife, Sharon, and my two daughters, Rachel and Grace; my parents for instilling in me a true love of learning. I would like to thank my fellow Ph.D. students (especially Fang Chu, Art Hendela and Linda Plotnick), my wonderful friends (especially Dough Finke, Barbara Boxer, Michael Pogozelski, Maria Stansberry, Caroline O'Connor, Don Becker, and Jim Miller) and the entire faculty in the Information Systems Department (especially Michael Bieber, Brook Wu and Julian Scher) for their inspiration, encouragement and guidance throughout this process. A very special thank you to the colleagues that participated in all three rounds of my research study: Melissa Thier, Himmat Singh, Venu Bolisetty, Jonathan Cavell, Chi Cheng, Robert Wu, Tim Boomer, David Winig, and John Kaczala. This work would not have been possible without the generous financial support of Edison Properties L.L.C., Gupton Marrs International and Lab49.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

Chapter **Page**

TABLE OF CONTENTS
(Continued)

Chapter **Page**

TABLE OF CONTENTS
(Continued)

Chapter **Page**

TABLE OF CONTENTS
(Continued)

Chapter **Page**

LIST OF TABLES

LIST OF TABLES
(Continued)

Table **Page**

LIST OF FIGURES

CHAPTER 1

OVERVIEW

1.1 Introduction

A constantly evolving regulatory environment, increasing market pressure to improve operations, and rapidly changing business conditions are creating the need for timely and ongoing assurance that organizational risks are continually and adequately identified and mitigated. These needs are paramount especially in large multinational corporations with highly distributed operations, extremely complex operating environments, and massive volumes of data, transactions, risks and controls that require review. Organizations are continually exposed to significant errors, fraud and/or inefficiencies that can lead to significant financial loss and increased levels of operating risk. The larger and more complex the organization, the greater these Enterprise Risks are (Coderre 2005).

An unmitigated Enterprise Risk can quickly grow into a full blown and far-reaching financial crisis, which is a long-standing and pervasive problem for capital markets and society as a whole. Reinhart and Rogoff chronicled financial crises over eight millennia that occurred in 66 distinct countries (Reinhart and Rogoff 2011). Moreover, business complexity has increased six-fold in sixty years; and, organizational complexity in terms of structures, processes and systems has increased by a factor of thirty-five (Morieux and Tollman 2014). During the same period, some have suggested that risk management has not evolved as quickly. The limited complexity and information richness currently used by internal auditors is woefully inadequate to model complex, information rich, global and highly dynamic markets (Redman and Hay 2012).

Unfortunately, these antiquated risk management procedures afford only a limited evaluation of an organization's business processes and Enterprise Risks. In today's hyper-complex and highly integrated operating environments, these risk management techniques are becoming increasingly inadequate as a preventative measure for a financial crisis.

Increasingly, technology is being harnessed to reinvent and improve risk management processes. Recent advances in Information Systems, artificial intelligence and modeling techniques have enabled sophisticated risk analysis. One particularly promising application of this technology is Continuous Auditing, which seeks to transform the audit process from periodic reviews of a few transactions to a continuous review of all transactions. However, today's highly integrated, rapidly changing and hypercompetitive business environment spawns numerous Enterprise Risks that historically have been excluded from typical internal risk management processes (e.g., surprise competitive threats, theft of sensitive customer data and supply chain failures). These high-value risks pose a material threat to today's corporations, which perhaps exceed the danger posed by fine-grain transactional risks that Continuous Auditing is predominately being used for at this time.

An extension of Continuous Auditing is referred to in this study as Continuous Monitoring, which is used by management to continually review business processes for unexpected deviations. Continuous Monitoring, like Continuous Auditing, requires a comprehensive understanding of an organization's business processes as well as their potential failure modes, key control points, rules, metrics and exceptions. When the process of identifying potential risks is automated, organizations are able to perform risk

assessments in real time, analyze business processes for anomalies and utilize data-driven indicators to identify emerging risks, which should help management make informed decisions, mitigate material risks and, hopefully, help prevent the next financial crisis. This research study will seek to understand which Enterprise Risks are most amenable to Continuous Monitoring techniques.

1.2 Research Problem

Whether or not Continuous Monitoring can be effectively used by management to monitor Enterprise Risks remains an open research question. Some believe that there are sizable benefits to extending the use of Continuous Monitoring applications. For example, one of the Office of Financial Research's key 2014 research objectives is to identify, assess and monitor potential threats to the United States' financial stability by developing tools that will monitor quantitative metrics and qualitative surveillance (Berner 2013). However, there are numerous obstacles: 1) replacing human judgment tends to be difficult, costly and computationally intensive; 2) large-scale Continuous Monitoring systems could be resisted because of their inscrutable complexity and novelty; 3) people and organizations may fear Continuous Monitoring because it erodes their competitive advantage and powerbase.

To determine whether this is a viable approach, I will explore the research question: What are the most potentially fruitful Enterprise Risks and a plausible technical architecture to support these implementations?

By using a Delphi, I will seek to drive expert consensus on the desirability and feasibility for applying Continuous Monitoring techniques to Enterprise Risks. The ultimate goal of this research is to provide a solid foundation for Continuous Monitoring

implementations that drastically improves an organization's risk management processes by pulling from the Continuous Auditing, Enterprise Risk Management, and Information Systems literature.

Figure 1.1 Blends three distinct disciplines.

1.3 Significance of this Research

Currently, the conditions that could lead to another major corporate catastrophe may not be fully known or understood at the appropriate level within a corporation, until it is too late to take meaningful action. This is due to the complex and integrated dependencies between corporations and the sheer number of potential Enterprise Risks they face. Continuous Monitoring's key objectives are to quickly detect a risk, assess its potential magnitude, and route it to the appropriate party for remediation, thereby reducing the probability of a corporate catastrophe.

Continuous Monitoring has the potential to improve an organization's Enterprise Risk Management processes, thereby reducing the probability of crisis resulting from an organization's unmitigated risks. However, Continuous Monitoring can only be effective

in this regard; if it is widely adopted and trusted by management throughout the enterprise.

With the ultimate goal of preventing the next crisis, this research study seeks to identify the Enterprise Risks that are most amenable to Continuous Monitoring, provide an architectural framework for future Continuous Monitoring implementations, and, most likely, identify future research opportunities within the domain of Continuous Monitoring. To that end, the following four research questions were studied:

- RQ1: What individual and organizational characteristics are related to the likelihood of favorable opinions toward the adoption of Continuous Monitoring?
- RQ2: Which Enterprise Risks are most amenable to Continuous Monitoring?
- RQ3: Which Continuous Monitoring architectural components are perceived as most applicable to which types of Enterprise Risks?
- RQ4: How does participation in an online Delphi process change the initial viewpoints of the participants?

The research methodology was a three-round Collaborative Design Delphi targeting professionals with experience in risk management, accounting and/or Information Systems. The Round 1 questionnaire had a consent form, demographic questions and scenario generation questions. Round 2 presented the three most auspicious risk scenarios from Round 1 and had participants evaluate the desirability and feasibility of using Continuous Monitoring on these risk scenarios. Round 3 presented the key assumptions collected in Round 2 and let the participants re-evaluate their desirability and feasibility answers from Round 2.

1.4 Organizational Structure

The rest of the dissertation is organized as follows: Chapter 2 provides a brief literature review for Enterprise Risk Management. Chapter 3 is a literature review for Continuous Auditing and Monitoring. Chapter 4 surveys the enabling Information System technologies for Continuous Auditing and Monitoring systems. Chapter 5 lays out a research agenda and methods. Chapter 6 presents the results of this Research Study. Chapter 7 summarizes this research study's findings and lists some research questions that could be addressed in future studies.

CHAPTER 2

ENTERPRISE RISK MANAGEMENT

2.1 Definition

Enterprise **R**isk **M**anagement (ERM) is a top-down risk-based approach to strategically manage a broad spectrum of corporate risks at the enterprise level. ERM is conceptually similar to corporate risk management, business risk management, holistic risk management, integrated risk management and strategic risk management, although each of these terms has a slightly different nuance (D'Arcy 2001).

Casualty **A**ctuarial **S**ociety (CAS) defines ERM as "a discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purposes of increasing the organization's short- and long-term value to its stakeholders." This definition highlights ERM's value creation as well as risk mitigation aspects. The corporation defines a top down process that methodically evaluates all plausible risks and considers their effect on all the relative stakeholders (CAS 2003, p. 8).

The **C**ommittee of **S**ponsoring Organization (COSO) of the Treadway Commission's ERM definition is "a process, affected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." This definition highlights ongoing and strategic process flowing throughout the entire corporation and affecting people at every level. This process is

designed to identify events that, if they occur, could materially affect the organization, achieve one or more separate but overlapping objectives, and provide reasonable assurance to the corporation's management (COSO 2004, p. 2).

(Makomaski 2008) simply and succinctly defines Enterprise Risk Management as a decision-making discipline that addresses variation in company goals. Alviniussen and Jankensgård define ERM as a holistic and company-wide approach (i.e., not a silo-approach) to managing risks and centralizing information in a Risk Universe (Alviniussen and Jankensgård 2009). They draw insights from modern portfolio theory that suggests that risks should be measured and managed on a portfolio basis and balanced against potential rewards, as well as from financial theorists that point out financial distress generally entails costly consequences. Consequently, an effective risk management program derives tangible business value by avoiding the costs associated with financial distress.

2.2 History

In 1654, the precursors to modern risk management were established when Pascal and Fermat discovered the basics of probability. By 1725, mathematicians were devising tables of life expectancy and marine insurance emerged as a legitimate business in England. In 1730, Abraham de Moivre discovered two essential ingredients for quantifying risk: standard deviation and normal distribution. In 1875, Francis Glaton discovered regression to the mean. In 1952, Harry Markowitz pioneered modern portfolio theory (Bernstein 1996).

In the 1950s, the risk management field was formalized by a group of insurance professors. The first risk management book was Risk Management in the Business

Enterprise. The basic premise was to maximize the productive efficiency of the corporation by managing risks in a comprehensive manner, and not simply insure them (Mehr and Hedge 1963).

In the 1970s, financial risk (e.g., foreign exchange risk, commodity price risk and equity risk) became an important source of organizational risk. Therefore, tools were developed for handling them (e.g., foreign currency futures, commodity futures contracts, and equity options). These tools usage accelerated during the next two decades and their misuse led to some exorbitant losses: Orange County ($1.5 Billion), Barings Bank ($500 Million), and Procter & Gamble ($157 Million) (Razali and Tahir 2011). In the 1990s, operational risk management emerged when shareholders began pressuring corporations to proactively mitigate risks rather than simply buying insurance for them. In the wake of various major corporate scandals and bankruptcies resulting from poor risk management, the United States government passed the Sarbanes-Oxley regulation in 2002, which mandates a top down risk assessment. Shortly thereafter, ERM was defined by CAS (Dionne 2013).

2.3 Process

At a high-level, there are two main potential Enterprise Risk Management processes described in the literature: CAS and COCO. CAS defines the high-level ERM process as follows: establish context, identify risks, analyze/quantify risks, assess/prioritize risks, treat/exploit risks, and monitor and review the process (CAS 2003). There are eight components of the COSO Integrated Framework:

1. Internal environment which refers to risk management philosophy, risk appetite, integrating of ethical values and the working environment of an enterprise

2. Objective setting which should be aligned with corporate vision and risk appetite
3. Event identification
4. Risk assessment that measures the frequency and impact of potential losses
5. Risk response is how a corporation mitigates risks. It may include avoidance, acceptance, and transfer of risk to and external entity
6. Control activities ensure the effectiveness of the risk management implementation
7. Information and communication disseminates program information throughout the corporations
8. Monitoring ensures that all risk management measures are appropriate and effective in mitigating risks (COSO 2004).

2.4 Benefits of Enterprise Risk Management

ERM should promote top-down risk awareness, which facilitates better operational and strategic decision-making. Some believe that ERM will become the new minimum standard for risk management, the key to survival for many companies and a significant source of competitive advantage (Stroh 2005). The following summarizes the key benefits described in the literature.

- (Berinato 2004) asserts that corporations that adopt ERM have fewer failed business ventures and incur less costs due to adverse events. (Heng Yik, Jifeng et al. 2011) showed that insurers with the best ERM programs had lower stock volatility and higher profitability as compared to those of their non-ERM or weak ERM peers.
- (COSO 2004) states that the benefits of its framework are improved capital deployment, tighten alignment between strategy and risk, increased opportunity to seize opportunities and reduced operational surprises.
- (Cumming and Hirtle 2001) state that ERM enables corporations to allocate capital efficiently among their business units and improves financial disclosures by providing a consistent and comprehensive assessment of the corporation's risk exposure.

- (Hoyt and Liebenbergerg 2008) found a positive relationship between United States Insurers' market value and the use of ERM. The ERM premium was roughly 20%, which is both statistically and economically significant.
- (KPMG 2011) states that corporations that have ERM processes tend to better understand their business risk profile and are often more proactive in heading off threats, and, rapidly surfacing and evaluating opportunities.
- (Lindberg and Seifert 2011) explains how ERM can aid with Dodd-Frank compliance.
- (Nocco 2006) speculates that ERM creates shareholder values by improving the mechanism to quantify and manage a corporation's risk-return tradeoff
- (Meulbroek 2002) determines that ERM increases corporate valuations, decreases financial distress costs, and reduces external monitoring and capital costs.

2.5 Adoption

There are many reasons a corporation may adopt ERM. Paape and Speklé found a corporation's regulatory environment, internal factors, ownership structure, and, firm and industry-related characteristics influence the choice to adopt ERM (Paape and Speklé 2012). For non-financial corporations (Alviniussen and Jankensgård 2009) determine the main motivations for implementing ERM (listed in order from the most cited to least) are improving corporate governance, improving compliance, mandate by board of directors, increasing shareholder value, improving decision marking, and following good business practices. Once a corporation decides to implement ERM they should adopt a Risk Taxonomy, ERM Framework and Best Practices, which are described in the following subsections.

2.5.1 Risk Taxonomy

There are numerous types of risks that can be incorporated into an ERM. However, the list below describes the risk taxonomy that is most frequently associated with ERM literature:

- Compliance Risk: Risk of violations or non-conformance with laws, rules, regulations, prescribed practices or ethical standards (OCC 1998).
- Financial Risk: Risk of loss due to economic conditions. For example, Credit Risk is the risk of an obligor's failure to meet the terms of a contract; Foreign Exchange Risk is the risk arising from movement in foreign exchange rates; Liquidity Risk is the inability to meet obligations when they come due, without incurring unacceptable losses; Price Risk is the adverse changes in the value of portfolios of financial instruments (OCC 1998).
- Strategic Risk: "Risk to earnings or capital arising from adverse business decisions or improper implementation of them. This risk is a function of the compatibility between an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against them, and the quality of the implementation of those decisions" (OCC 1998, p. 5).
- Operational Risk: Risk of inadequate or failed internal or external processes, people and systems (Basel 2001)

2.5.2 ERM Frameworks

There are a number of ERM frameworks that are currently being used. The most frequently cited are:

- A Risk Management Standard by the Federation of European Risk Management (FERMA).
- Australia/New Zealand Standard 4360-Risk Management.
- Basel.
- COSO's Enterprise Risk Management-Integrated Framework.
- King ll Report by The Institute of Directors in Southern Africa (IoDSA).
- Internal Control: Guidance for Directors on the Combined Code (i.e., Turnbull Report).

- The Institute of Management Accountants' (IMA) "A Global Perspective on Assessing Internal Control over Financing Reporting" (ICoFR).

Although these standards may differ in name, industry and region, they all identify, prioritize and quantify risks in order to help corporations effectively manage their exposure (Yazid, Hussin et al. 2011)

2.5.3 Best Practices

The literature describes several best practices that have been adopted by successful ERM implementations. (Lawrence 2005) describe ten best practices for an ERM implementation:

1. Engage senior management and board.
2. Create an independent ERM entity under the Chief Risk Officer.
3. Impose a top-down governance structure.
4. Select an ERM framework suitable for the corporation's key risk.
5. Establish a risk aware culture.
6. Disseminate written policies with risk limits and business boundaries.
7. Create an ERM dashboard that integrates key quantitative and qualitative risk metrics.
8. Use risk analytics to measure risk concentrations and interdependencies.
9. Integrate ERM into strategic planning, business processes and performance measurement.
10. Optimize for risk-adjusted profitability.

(Barton, Shenkir et al. 2009) suggest the following seven best practices:

1. Integrate the ERM process into the corporation's strategy.
2. Understand the corporation's risk appetite.
3. Understand the corporation's major risks.
4. Ensure corporate governance is strong.
5. Develop meaningful risk metrics.
6. Link compensation to risk.
7. Do not dismiss high impact low probability risks.

2.6 Challenges

ERM has not been universally adopted. Beasley and Clune survived senior accounting executives, which revealed only 20% currently had an ERM in their corporation and 29% had no plans to implement one (Beasley, Clune et al. 2005). Negus highlights ten common ERM implementation challenges: Assessing ERM's value, balancing risk visibility with legal exposure, defining risk, selecting a risk assessment method, assessment metrics and time horizon, understanding a risk's multiple event likelihoods and severities, ERM ownership (i.e., determining what internal group champions the ERM effort), risk reporting (i.e., determining what information should be shared with whom), simulations and stress tests (i.e., balancing the needs for meaningful simulation with the near infinite number of potential scenarios) (Negus 2010).

In September 2008, (Beasley, Branson et al. 2009) surveyed more than 700 corporations, whose revenue ranged from $15 thousand to $115 Billion. The main barriers to ERM implementation were competing priorities, insufficient resources, lack of perceived value, lack of executive leadership, incremental bureaucracy, and legal or regulatory barriers.

CHAPTER 3

CONTINUOUS AUDITING AND CONTINUOUS MONITORING

3.1 Definitions

Global **T**echnology **A**udit **G**uide (GTAG) defines Continuous Auditing as a process to ensure that the policies, procedures, and business processes are operating effectively, which includes defining the control objectives and assurance assertions and establishing automated tests to highlight activities and transactions that fail to comply. They also define several related processes:

- Continuous Control Assessment: a process that focuses on the early detection of control deficiencies.
- Continuous Risk Assessment: a process that detects processes or systems that experience higher than expected levels of risk (Coderre 2005).
- Continuous Monitoring: a process to ensure that the policies, procedures, and business processes are operating effectively, which includes defining the control objectives and assurance assertions and establishing automated tests to highlight activities and transactions that fail to comply.

Deloitte's definition of Continuous Auditing and Continuous Monitoring adds the nuance that Continuous Auditing is used by internal audit to continually gather data that supports their auditing activities while Continuous Monitoring is used by management to continually review business processes for unexpected deviations (2010). Continuous Monitoring, per the above Deloitte definition, is related to Continuous Auditing.

The Canadian **I**nstitute of **C**hartered **A**ccountants (CICA) and the **A**merican **I**nstitute of **C**ertified **P**ublic **A**ccountants (AICPA) define Continuous Auditing as "a methodology that enables independent auditors to provide written assurance on the subject matter using a series of auditor's reports issued simultaneously, or within a short

time after the occurrence of the events that underline the subject matter" (CICA/AICPA 1999, p. xiii) Rezaee defines Continuous Auditing as "a systematic process of gathering electronic evidence as a reasonable basis to render an opinion on fair presentation of financial statements prepared under the paperless, real-time accounting system" (Rezaee 2001, p. 151). Helms and Mancino define Continuous Auditing as "software to detect auditors specific exceptions from all transactions that are processed either in real-time or near real-time environments. These exceptions could be investigated immediately or written to an auditor's log for subsequent work" (Helms, Mancino et al. 1999, p. 62). Although the above definitions differ in semantics and scope, they all share the notion of performing auditing processes quickly and continuously.

3.2 History

Accounting practices have been around for a very long time. In the Mesopotamia, circa 3500 BC, scribes, the forerunners of modern day accountants, would record the terms of financial transactions on tamper-resistant clay tablets (Alexander 2002). In the United States, contemporary accounting practices emerged in the 19th century when accounting professionals applied quantitative methods to assess the amount, timing and certainty of a corporation's future cash flows (King 2006). Over time, these accounting practices have amassed a comparatively cheap and plentiful workforce, ingrained themselves into contemporary business processes, and proven generally reliable, flexible and independent from underlying information technology (Weber). Perhaps motivated by their own self-interest, several influential accounting professionals are highly skeptical that these practices need to be drastically changed (Whitehouse 2010).

Cash is generally credited with the seminal article that laid the foundation for the Continuous Auditing domain space. Cash and Bailey describe various procedures to validate the correctness of **E**lectronic **D**ata **P**rocessing (EDP) systems and **T**he **I**nternal **Co**ntrol **M**odel (TICOM) (Cash Jr, Bailey Jr et al. 1977). This model enables the automation of testing an organization's internal control system. He envisioned that the organization's internal control would be stored in a database. Vasarhelyi and Halper coined the term Continuous Auditing when they described the process used at AT&T Bell Labs to audit a large paperless billing system in real-time (Vasarhelyi and Halper 1991). This paper describes the key building blocks of a Continuous Auditing system: extracting audit data from a system, using it to calculate operational analytics that are compared to standard metrics, generating alarms that alert an auditor to potential issues and generating audit reports.

3.3 Process

The Continuous Auditing literature describes many different processes. Chan and Vasarhelyi defines a basic Continuous Auditing process, which is a four-stage process. Stage 1 automates data capture. Stage 2 uses data modeling of historic transactions and account balances to create benchmarks. Stage 3 uses these benchmarks to evaluate internal controls, transactions and account balances. Stage 4 investigates only the benchmark exceptions. If no exceptions are discovered, the financial information is deemed to be free of material errors, omissions and fraud (Chan and Vasarhelyi 2011).

Figure 3.1 Basic continuous auditing process.

(Coderre 2006) puts forward a five-step process to continuously analyze audit data:

1. Define Objectives, which includes identifying key Information Systems and data sources, and understanding the business processes and application systems in place.
2. Determine Data Access and Use, which includes selecting analysis tools, developing analysis capabilities, auditor analysis skills and techniques, and assessing integrity and reliability of the data.
3. Perform a Continuous Control Assessment, which includes identifying critical control points, defining control rules, defining exceptions, and designing an approach to test controls and identify deficiencies.
4. Perform a Continuous Risk Assessment, which includes defining entities to be evaluated, identifying risk categories and identifying data-driven indicators.
5. Report and Manage Results, which includes prioritizing results, identifying control deficiencies or increased levels of risk, initiating appropriate audit response, providing results to management, evaluating the results of the actions taken, and monitoring and evaluating the effectiveness and security over the whole process.

(Fedorowicz 2008) has a five-step process:

1. Identify the full range of risks.
2. Establish a risk management culture.
3. Align controls with risks embedded in the business processes.
4. Devise procedures for manual interventions.
5. Consolidate and track controls used in the auditing process.

(Rezaee 2002) suggests a ten-step process:

1. Define audit objectives.
2. Understand business rules.
3. Identify key business data.
4. Obtain data.
5. Identify data elements.
6. Establish data access.
7. Extract data.
8. Create Audit Meta-data.
9. Load Audit Data.
10. Execute Audit Test Scripts.

3.4 Benefits

Several different studies and research reports have listed a wide array of potential benefits from a well-functioning Continuous Auditing system. A Deloitte report (2010) lists the following benefits that could result from a Continuous Auditing system: improved risk and control assurance, reduced audit costs, increased audit effectiveness, reduced audit cycles, identifying control exceptions in real time by replacing manual preventative controls with automated detective controls, and increased competitive advantage and shareholder value. A Gartner research report written by (Caldwell and Proctor 2010) states that the primary market drivers for Continuous Auditing are regulatory compliance, risk management and business performance. In September 2008, the Economist asked 446 senior executives what their views were on the expected benefits from standardizing/automating their financial processes. The list of expected benefits include (listed from most frequently cited to least frequently cited): cutting back

on error prone manual processes, enhancing data integrity, allowing employees to focus on high value activities, reducing costs, institutionalizing standard processes across the enterprise, improving productivity, increasing process visibility, and enhancing compliance with regulatory requirements (Fedorowicz 2008). In one specific example (Brennan 2008), who has implemented Continuous Auditing techniques at Siemens, lists the following benefits that his organization has received from Continuous Auditing: audits get deeper and broader, audits take less time, improve communication with external auditors and key controls are rationalized. The following subsections explore some of the potential benefits of a Continuous Auditing in more detail.

3.4.1 Reduced Costs

Several cost savings are associated with Continuous Auditing, which automates the auditing of business processes. First, Continuous Auditing continually and automatically monitors control effectiveness, which eliminates the labor-intensive and repetitive re-testing of controls by obviating the need to re-perform most if not all point-in-time audits. Second, placing the requisite audit data in a central repository that can be remotely accessed obviates the need for traveling to remote locations to perform site audits. Third, external auditor's fees would be ideally eliminated or, at least, sharply reduced because the Continuous Auditing systems would automatically perform most, if not all, of the auditing and assurance processes.

A study by (Wallace 1984) concluded that shifting audit responsibility to internal auditors and away from external auditors reduces the total auditing cost for an organization. Reducing the cost of the audit and monitoring processes is especially germane because budgetary constraints on these functions have perpetually become more

stringent. These cost savings can be quantified and compared to the cost of implementing a Continuous Auditing system. However, other advantages of automation such as enhanced data integrity, fewer instances of noncompliance, better business decisions and risk management and reduced fraud risk are harder to quantify.

3.4.2 Improved Audit Quality

There are several ways that Continuous Auditing could improve audit quality. Means and Warren point out the limitations of the traditional auditing model, which relies on the presence of internal controls and sampling (i.e., the periodic checks of selected controls) (Means and Warren 2005). Much of the traditional audit process must be done manually in order to examine the effectiveness of a corporation's internal controls. However, Continuous Auditing advances make plausible a new and better audit approach that continuously checks all of an organization's financials and related transactional data, and perpetually searches for audit anomalies or outright fraud. Generally speaking, Continuous Auditing systems detect audit exceptions quickly and notify the appropriate parties so corrective action can also be taken quickly.

Several studies illuminate the foibles of human decision making that detract from audit quality. Since Continuous Auditing systems do not share these biases, these systems could presumably perform better and more objective audits. Bazerman and Loewenstein suggest that auditors cannot be totally objective because of an innate self-serving bias (Bazerman, Loewenstein et al. 2002). They tend to discount facts contradicting their preferred position and uncritically embrace evidence supporting it. He lists several reasons for this: ambiguity (auditors tend to reach for self-serving conclusions whenever ambiguity surrounds evidence), attachment (auditors are highly

motivated to remain in a client's good graces), and approval (auditor may accept a more aggressive accounting position from clients than they themselves would recommend).

Just like all human beings, auditors suffer from the foibles of human decision-making. Hammond and Keene states eight psychological traps that may lead to bad decision-making:

1. The status quo trap: biases towards maintaining the current situation even when better alternatives exist.
2. The sunk cost trap: the tendency to justify past decisions.
3. The evidence trap: the tendency to search for information supporting an existing predilection and to discount opposing information.
4. The framing trap: undermining the entire decision-making process by misstating the problem.
5. The overconfidence trap: overestimating the accuracy of our forecasts.
6. The prudence trap: tendency to be overcautious when estimating uncertain events.
7. The recallability trap: the tendency to give undue weight to recent and dramatic events.
8. The anchoring trap: the tendency to give disproportionate weight to the first information received (Hammond, Keeney et al. 2001).

(Smith and Kida 1991) confirms that auditors do fall prey to the anchoring trap however, expert auditors performing familiar job-related tasks are less likely to fall into the anchoring trap than the control groups were.

As an organization's scale and scope of operations increases so does the complexity of its business transactions, risk exposure, and, scale and scope of their audit procedures. Since manual audit procedures do not scale well, once an organization reaches a sufficient size these audit procedures become prohibitively expensive and time-consuming to execute. On the contrary, Continuous Auditing tends to be highly scalable.

Consequently, it may be the only viable alternative for today's largest global organizations.

3.4.3 Compliance with Laws and Regulations

Public Organizations are forced to comply with many different laws and regulations however, the cost to comply with these laws and regulations is staggering. For example, United States-based companies must comply with the **S**arbanes-**Ox**ley (SOX) Act of 2002, which was enacted in the wake of a number of major accounting scandals including the collapse of Enron, Tyco International and WorldCom. A study conducted by **F**inance **E**xecutives **I**nternational (FEI) indicated that for 185 companies with average revenues of $4.7 billion, the average compliance costs were $1.7 million (FEI 2008). Section 404 of Sarbanes-Oxley Act of 2002, which requires management and the external auditor to report on the adequacy of a company's internal controls, is the most costly aspect of the legislation for companies to implement because documenting and testing important financial controls requires enormous effort (Mehra 2006). Moreover, most organizations have additional compliance costs such as producing audited financial statements, which requires an independent auditor to attest to the accuracy and completeness of their financial statements.

There is a clear trend toward increasing and constantly evolving regulatory requirements. For example, in the banking industry the Basel I accord, which was ratified in 1988, influenced banks residing in G-10 countries behavior by proscribing capital ratios (Jablecki 2009), which was replaced by Basel II in June 2004, and Basel III (Moody's 2012). In July of 2010 when the Dodd-Frank legislation was signed into law, the banking industry received a whole new wave of regulations. This act was billed as

the most sweeping overhaul of the United States financial regulatory system since the Great Depression (2009) and was responsible for roughly 300 new regulatory requirements affecting many different lines of business for financial institutions (Protess 2011). For example, it limits abusive lending practices, fees for debit-card usage and high-risk bets on complex derivative securities, creates a bureau to protect consumers from financial fraud, and provides a means for the government to supervise the largest financial institutions under the guise of avoiding catastrophic financial failure (2011).

Clearly, these new compliance requirements will increase these organizations' compliance expense. For example, Basel II, which is an international standard that regulates how much capital banks need to put aside to guard against financial and operational risks, has three Pillars. Pillar 1 quantifies the bank's credit risk (i.e., the risk of a loss due to a debtor's nonpayment of a loan or other line of credit) and operational risk (the risk of loss from a bank's business functions including fraud risk and environmental risks) to calculate the capital requirements for international banks. These capital requirements aim to ensure that international banks have sufficient capital to meet their requirements, cover unexpected losses and promote public confidence. In general, the greater the bank's risk, the greater its capital reserves must be. Pillar 2 describes the requisite management obligations in evaluating the bank's corporate governance, risk management and risk profiles that are not explicitly covered by Pillar 1. Systemic risk (i.e., the risk of loss due to a collapse of the entire financial system or market), concentration risk (i.e., the risk of loss due to the concentration of a bank's outstanding accounts relative to the total number of debtors that the bank has lent money to) and liquidity risk (i.e., the risk of loss resulting from being unable to trade a security or asset

quickly) are some of the residual risks that are addressed in Pillar 2. Pillar 3 explains transparency and disclosure requirements. Specifically, stakeholders should have sufficient understanding of the bank's activities and risks to make informed decisions about the bank's overall risk position (2006). The Office of the Comptroller of the Currency estimates that if all nationally chartered banks were to adopt Basel II, the combined compliance costs would be nearly $1.1 billion, or almost $680,000 per bank (VanHoose 2007).

There have been several journal articles that suggest Continuous Auditing could help organizations reduce their cost of compliance. Means and Warren discusses how new software that continuously extracts data from enterprise systems can perform a broad range of auditing, fraud tests and anomaly identification (Means and Warren 2005). Vasarhelyi asserts that Continuous Auditing techniques may assist in Sarbanes-Oxley compliance by providing evidence that controls are functioning and furthermore provide an understanding of the consequences of ineffective or non-operational controls (Vasarhelyi 2004). While this software may never totally replace manual auditing, many speculate that it could cost-effectively perform many traditional auditing tasks.

3.4.4 Reduced Risk

Companies that quickly make high-quality decisions and implement them effectively generally beat out rivals (Blenko and Mankins 2012). Conversely, according to a Booz Allen report, the biggest threat to shareholder value over the past ten years was overly risky decisions made by senior management. They cost more shareholder value than other audit issues such as fraud, ethics violations or rogue traders (Ovans 2012). This claim is supported by a (ORX 2012) report that states its consortium of financial service

firm's biggest loss category was "Execution, Delivery and Process Management", which accounted for 32% of their total loss or €4.8 billion in 2011. Although the supporting research is sparse, Continuous Auditing seeks to drastically improve the organizational decision and risk management processes by augmenting and checking human decision-making. Therefore, it's plausible that Continuous Auditing could improve organizational decision-making and reduce the number of associated loss events, thereby directly improving the organization's bottom line.

In 2008, the Association of Certified Fraud Examiners estimated that United States organizations lost 7% of their annual revenues, approximately $994 billion, to fraudulent activity. Even more troubling, internal and external audits and internal controls detect only 23.3% of all fraud. Fraudulent financial statements had the highest median loss of all fraud schemes with a median loss of $2 million per incident (Ratley 2008).

Opinions vary on how effective Continuous Auditing would be in detecting fraudulent financial statements, which is generally perpetrated by executives of an organization. Vasarhelyi, and Kogan asserts that a well performed Continuous Audit would have detected Enron's fraudulent accounting improprieties, because the continuous assurance process would have triggered alarms that would have been difficult for Enron's operational managers, auditors and top management to ignore (Vasarhelyi, Kogan et al. 2002). However, Krass argues that Continuous Auditing probably would not prevent fraud that is perpetrated at the highest levels of an organization, which was the case with Enron (Krass 2002).

There is a growing body of research that suggests Continuous Auditing could be a valuable tool in preventing some types of fraud schemes. Lin used a fuzzy neural network to assess the risk of fraudulent financial reporting for an organization (Lin 2003). Using publicly available metrics such as allowance for doubtful accounts as a percentage of net sales and accounts receivable, ratio of gross margin to net sales, net sales, accounts receivable and allowance for doubtful accounts, this model was able to successfully detect fraud 35% of the time, which was better than the logistic regression model that only had a 5% detection rate. Baker and McCollum explain how machine learning technologies such as inductive logic programming and neural nets are helping organizations such as Bank Itau and Sun Trust Bank detect suspicious activity and mitigate the risk of fraudulent transactions (Baker and McCollum 2005). Viaene and Derrig investigate the explicative capabilities of three classification algorithms (neural nets, decision trees and logistical regression) in detecting fraudulent automobile claims that occurred in Massachusetts during 1993 (Viaene, Derrig et al. 2002).

(Eining 1997) compared three decision aids (checklist, logistic regression and expert systems) on their ability to help auditors detect fraudulent reporting. He concluded that auditors that used expert systems made better decisions that were more consistent with their assessment of risk than did auditors that used either checklists or logistic regression, or no decision aids. Kuhn and Sutton describe how Continuous Auditing techniques could have been used to detect WorldCom's business transactions that did not conform to Generally Accepted Accounting Principles (GAAP) and consequently overstated WorldCom's revenues (Kuhn and Sutton 2006).

There are many other types of risks that plague corporations. For example, one recent Delphi study, using 37 professionals, identified 86 separate threats in 11 different categories that potentially are important for the next decade (Turoff 2012). Most of these threats would materially and adversely affect the corporation's ability to operate normally.

3.4.5 More Frequent Audited Disclosures

Electronic commerce, electronic data interchange and the Internet are dramatically changing an organization's business practices for record keeping. As more of an organization's record keeping becomes digitized, the processes of collecting audit information, assuring its accuracy and disseminating financial reports to stakeholders can be highly automated. The automation of the financial reporting process could enable financial reports to be released more frequently. Currently, most companies release unaudited financial reports quarterly and audited financial reports annually. However, increasingly stakeholders require more timely communication of financial information, which requires auditors to invent new ways to continuously monitor, gather and analyze audit evidence (Rezaee 2002).

An experiment conducted by (Hunton 2002) demonstrated the potential value of more frequent financial reporting. He concludes that monthly financial reporting even without assurance (i.e., unaudited), would significantly enhance the usefulness of financial statements, improve the quality of earnings, reduce managements' aggressiveness with respect to accounting accruals and estimates, reduce stock price volatility, improve analyst consensus of future earnings estimates and reduce the

organizations cost of capital. These effects were more pronounced if the monthly financial statements were accompanied by assurance (i.e., audited).

(Botosan 1997) examine the association between disclosure levels and the cost of equity by regressing estimates on an organization's cost of equity on market betas (i.e., its non-diversifiable risk) and firm size. Botosan's analysis of 122 manufacturing firms supports the theory that an increase in financial disclosures is correlated with a lower cost of equity. After controlling for market beta and the organization's size, the magnitude of the disclosure effect is negatively correlated with approximately 28 basis points change in the cost of equity. However, organizations that had the most financial analysts covering them had no significant relationship between disclosure levels and cost of equity capital.

(Elliott 2002) states the potential downside associated with more frequent disclosures of financial reports: the potential to place the organization at a competitive disadvantage, the high cost of developing, processing and distributing frequent financial reports, and the risk of liability from its disseminations. Moreover, a field study of three publicly traded firms reveals that only 10.6% of internal accounting professionals are receptive to making financial statements available to external users on a more frequent basis than quarterly and only 16.3% believe that the benefits of more frequent reporting would outweigh the costs, even though most accounting and information technology professionals believe that it is technically feasible to do so (Chan and Wright 2007).

Given the few audited disclosures, stock prices are routinely influenced by non-audited information, which at times can be of dubious quality. For example, microcap stocks, which notoriously lack publicly available audit information, have been plagued by numerous "pump and dump" fraud schemes. Fraud perpetrators use a variety of tactics

including spam, paid promoters, cold calling, and/or dubious press releases to artificially increase a company's stock prices ahead of their sell off (SEC 2014). More frequent and widely distributed audited information could lead to more efficient markets by impeding dubious information's ability to sway stock prices.

3.4.6 Improved Trust

(Power 1999) asserts that the United Kingdom is in the midst of an "Audit Explosion" because of a lack of trust. He suggests that auditing has been increasingly used to restore trust in situations where resources are entrusted but trust is lacking. However, all auditing has explicit costs. Societies that have tried to institutionalize auditing on a grand scale have slowly crumbled under the weight and cost of their information validation demands. The over-allocation of scarce resources to surveillance activities and the sheer human exhaustion of perpetual audit activities seem to outweigh their benefits. He asserts that the traditional audit process invests too heavily in shallow rituals of verification at the expense of other forms of organizational intelligence. The ultimate goal of an audit program should be to open up an organization to independent and external scrutiny thereby establishing broad-based trust, which obviates the need for costly auditing.

Some have provided examples that Continuous Auditing could improve organizational trust. Continuous Auditing systems could monitor service level agreements, contractual obligations and/or loan covenants between organizations, which should improve trust between counterparties. For example, (Coletti, Sedatole et al. 2005) suggests and provides evidence that control systems between organizations can increase trust and reduce risk of organizational collaboration such as strategic alliances and joint

ventures. Moreover, (Woodroof and Searcy 2001) describes a continuous debt covenant monitoring system that a lender could use to verify that a borrower complies with the covenant agreements.

3.5 Adoption

Many believe Continuous Auditing is the future of auditing. Continuous Auditing techniques can be applied to a wide breadth of domain spaces. On one extreme Continuous Auditing has been used in very specific and well-defined domains (e.g., WebTrust and SysTrust). WebTrust's sole purpose is to provide assurance on a website's privacy and consumer protection procedures, while SysTrust provides assurance on a website's security, availability and processing integrity (WebTrust.org 2009).

At the other extreme, Continuous Auditing could be the basis for an organization's enterprise-wide **G**overnance, **R**isk and **C**ompliance (GRC) program (Caldwell 2009). Gartner defines Governance as the process by which policies are set and decision-making is executed; Risk Management as the process for addressing risks by either mitigation through the application of controls, transference through insurance and/or acceptance through a governance mechanisms; and, Compliance as the process of adhering to policies that can be derived from internal directives, procedures and requirements or external laws, regulations, standards and agreements (Caldwell 2009). A full-blown GRC Continuous Auditing installation at an arbitrarily complex Fortune 500 company would be a gigantic endeavor.

On an even grander scale, (Hulstijn, Christiaanse et al. 2011) explain how Continuous Auditing could be used to ensure regulatory compliance through the entire value chain for the meat processing industry: (i.e., feed creation, cattle farm,

slaughterhouse, meat packing and retail). Hulstijn's example crosses several distinct and independent organizations that constitute the Netherlands' meat packing industry.

However, the adoption rate of Continuous Auditing has been slow. A KPMG survey indicated that fraud detection was the biggest factor driving adoption of Continuous Audit systems. The other drivers listed include: Enterprise Risk Management, Sarbanes-Oxley compliance, compliance with internal policies and procedures and regulatory compliance (2010). A 2003 survey of internal auditors conducted by the Institute of Internal Auditors Research found that 79.4% of the respondents used some form of computer assisted audit techniques and 39.9% use computer-based monitoring and exception reporting in their departments (Warren 2003).

(Baksa, Turoff et al. 2010) summarizes three successful Continuous Audit implementations at AT&T, RCMP and Siemens. Kent and Zahid speculate how Continuous Auditing could be embedded into health care systems (Kent, Zahid et al. 2011). The Financial Executive Research Foundation explored 11 successful Continuous Auditing implementations at American Electric Power, Blue Cross and Blue Shield of North Carolina, Chicago Mercantile Exchange, Hallmark Cards, Hewlett-Packard, IBM, Intel, Microsoft, J.C. Penney, United Technologies Corporation and Wells Fargo (Ramamoorti 2010).

The transition from traditional auditing techniques to Continuous Auditing is most likely going to be a slow evolution rather than a dramatic metamorphosis. Kuenkaikaew posits a four stage audit maturity model. In Stage 1 is the traditional audit, where assurance is predicated on financial reports presented by management (Kuenkaikaew 2008). In Stage 2 assurance is predicated on effective control monitoring. In Stage 3

assurance is predicated on verification of quantified controls and operational results. In Stage 4 assurance is provided by a Continuous Audit with a meta-control structure and audit by exception.

3.5.1 Success Criteria

A KPMG whitepaper (2010) defines several potential success criteria for a Continuous Auditing implementation. KPMG defines financial success criteria (e.g., positive financial return on investment for the project) as well as non-financial success criteria (e.g., improved employee compliance with policies and procedures). The positive return on investment could stem from a reduction in the Sarbanes-Oxley compliance costs, increase prevention of fraud, reduction in the labor costs required to complete an audit, and the cost savings associated with the enhanced ability to detect control failures quickly before they have the chance to escalate into a costly issue. Over the course of the Continuous Auditing system's lifecycle success metrics, such as the ones listed above, could be continually evaluated to determine the overall effect of this system on the organization.

(Krell 2009) offers the following five suggestions to improve the adoption of a Continuous Auditing implementation:

1. Establish highly visible executive support.
2. Communicate with business process owners to identify areas of greatest need (i.e., most important risks).
3. Start small in a specific area with receptive business process owners.
4. Understand that the technology will likely identify "false positives" on the first several cuts; weed these out as the application is iteratively optimized.
5. Communicate the errors and issues identified to business process owners in a consultative manner.

3.5.2 System Acceptance

In order for Continuous Auditing to become a mainstream application, it will have to overcome the system acceptance issues that plague all new information technology projects. Continuous Auditing could be used by many different stakeholders and may face resistance along many different fronts. The three biggest potential stakeholders are organizations, big accounting firms, and auditors (external and internal). Each of these stakeholders has individual needs and desires that will help shape their reaction to a Continuous Auditing system.

Also, for a Continuous Auditing system to be effective, it would not only have to be proficient at auditing, but it would also have to be trusted and relied on by its stakeholders. Trust in computer systems, especially new ones, can be problematic. For example, six months before 40 million credit cards were stolen from Target, it spent $1.6 million on a sophisticated and well-known anti-malware system that detected the attack and warned the appropriate personal, who took no action. In fact, this software could have automatically removed the malware without any human interaction. However, this feature was disabled, presumably because it was mistrusted by Target's security personnel, even though it was adequately tested both on Target's infrastructure as well as at numerous other companies (Riley, Elgin et al. 2014) (Smith 2014).

3.5.3 Organizational

Acceptance of an information technology system within an organization has been well documented in the Information Systems literature. Specifically, (Bailey James 1983) identified the five system attributes that lead to the highest user satisfaction with a computer system:

- Accuracy - The correctness of the system's output.
- Reliability - The consistency and the dependability of system's outputs.
- Timeliness - The output of information in a time suitable for its use.
- Relevance - The degree of congruence between what a user wants or requires and what is provided by the system.
- Confidence in the System - The user's feeling of assurance or certainty about the system.

Therefore, other things being equal, a Continuous Auditing system that exhibits a high degree of these attributes should be more accepted than one that ranks low on them.

(Venkatesh, Morris et al. 2003) developed and tested a Unified Theory of Acceptance and Use of Technology (UTAUT), which can be used as a starting point to understand the potential system acceptance issues that a Continuous Auditing system could encounter. Four constructs were identified as direct determinants of user intention and usage behavior:

- Performance Expectancy (the degree to which an individual believes that using the system will help him/her attain gains in job performance).
- Effort Expectancy (the degree of effort associated with using and learning the system).
- Social Influence (the degree to which an individual perceives that important constituents believe he or she should use the system).
- Facilitating Conditions (the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system).

Gender, age, voluntariness and experience are key moderators of these four direct determinants. Performance Expectancy is moderated by gender and age. This relationship is more significant for men and younger workers. The Effort Expectancy is moderated by gender, age and experience. This relationship is more significant for women and older workers, and those with limited experience. The Social Influence is contingent on all four moderators. This relationship is more significant for women, older

workers, under conditions of mandatory use, and those with limited experience. The effect of facilitating conditions is moderated by age and experience. This relationship was more significant for older workers and those with more experience (Venkatesh, Morris et al. 2003).

Consequently, UTAUT predicts high behavioral intention to use a new Continuous Auditing System when the end-users believe that the Continuous Auditing system is easy to use and well supported in terms of organizational and technical infrastructure, will improve their efficiency and effectiveness at work, and is supported by senior management. The prediction that a successful Continuous Auditing system implementation benefits from the support of an executive champion is consistent with the empirical research conducted by financial executives research foundation (Ramamoorti 2010).

3.5.4 The Big Four Auditing Firms

The big four accounting firms are PwC, Deloitte and Touche, Ernst & Young, and KPMG. Collectively in 2011, these firms had revenues of over $100 billion and employed over 640,000 employees. Table 3.1 summarizes this information.

Table 3.1 Big Four Auditing Firm's Revenue and Number of Employees

Audit	Revenue (in Billions)	Employees (in Thousands)	Fiscal Year	Reference
PWC	$29.2	169	2011	(Davies 2011)
Deloitte & Touche	$28.8	182	2011	(2011)
Ernst & Young	$22.9	152	2011	(2011)
KPMG	$22.7	138	2010	(Flynn 2011)
Total	**$103.6**	**641**		

Over the years, these large auditing firms have built a large and global industry, and amassed substantial intellectual property around performing traditional audits.

Historically, these firms have been resistant to new technologies that could potentially jeopardize their business model. For example, (Fischer 1996) observed that large auditing firms had a reluctance to place reliance on more sophisticated and/or effective audit procedures even when they were readily available. Their preferences tended to be anchored on the audit procedures and processes that have been performed in the past. Moreover, (Hall 2003) suggests that adoption of a new invention might be slowed if it requires new and complex skills. This inertia and resistance to new technologies could be a barrier to Continuous Auditing acceptance. Finally, the Big 4 audit firms may be resistant to Continuous Auditing's tenant of reviewing all the transactions, because this practice could complicate their legal defenses for overlooking a material financial misstatement.

(Dowling and Leech 2007) review of audit support systems may provide insight into the performance expectancy for a Continuous Auditing system from the perspective of the big audit firms. They conducted semi-structured interviews with four partners and four managers from five audit firms, which included a Big 4 and one mid-tier international audit firm. Continuous Auditing systems perceived benefits were enhanced audit quality, increased audit efficiency, higher audit consistency, better risk management, improved documentation and increased checks and balances on junior staff. On the contrary, their perceived limitations include fostering mechanistic behavior as opposed to judgment, significant training time, technology challenges, cost prohibitive for certain types of tasks, and perceived complexity.

One study suggests possible means to overcome these audit firm's inertia and initial resistance to new technologies. Curtis and Payne analyzed the acceptance in auditing firms of **C**omputer **A**ssisted **A**udit **T**echniques (CAATs), which leverages technology similar to what is used for a Continuous Auditing system (Curtis and Payne 2008). CAAT applies this technology within the context of a traditional periodic audit while Continuous Auditing uses this technology to perform audits on a continuous basis. He concludes that the acceptance of CAAT improves when superiors voice their approval for the new CAAT software, and longer-term budget and evaluation periods are used. Longer evaluation periods are necessary, because these implementations typically have high front-loaded costs. In the early periods, these startup costs more than outweigh the overall efficiency gains and improvements in audit quality. However, over time the system implementation and maintenance costs tend to dramatically decrease while the efficiency gains remain constant. For a well-designed system, the total economic benefits of the system tend to surpass its total costs in some future period.

3.5.5 Auditors

Using Continuous Auditing systems will require new skills, technical competencies and attitudes for both internal and external auditors. Continuous Auditing will require auditors to be open to adopt risk-based assurance principles and have a fundamental understanding of Information Technology concepts and methodologies. Specifically auditors need to be able to teach themselves new technical solutions, perform data extractions, use statistical analytical tools, and understand ERPs and mid-level accounting packages (Vasarhelyi, Teeter et al. 2010). The Unified Theory of Acceptance and Use of Technology theory predicts that auditors that have these abilities will have a

lower Effort Expectancy (see Subsection 3.5.3) for using Continuous Auditing systems. As such, they will be less resistant to this technology than auditors that do not have these skills.

Another potential reason that auditors might resist a Continuous Auditing system is, as automation increases audit efficiencies, there could be a corresponding decrease in the demand for auditors. Similar to the way machines reduced the demand for physical labor, some have argued that as machines take over mental labor, there will be a corresponding and irrevocable reduction in the demand for knowledge workers (Ford 2009). Applying this line of reasoning to the audit profession, if Continuous Auditing has large-scale success in fully automating the audit process, there could be a sharp decrease in demand for the traditional auditor's skill set. If auditors perceive a dire threat to their livelihood, they may staunchly resist the new system.

3.6 Challenges

Although Continuous Auditing implementations are occurring, their adoption is slower than expected (Warren 2003). Consequently, Continuous Auditing still has not been widely adopted in corporate America, in spite of the fact that audit experts and software vendors have touted its benefits for over a decade (Whitehouse 2010). However, one study showed that Continuous Auditing techniques are emerging in some internal audit departments, but much opportunity for additional proliferation (Vasarhelyi, Alles et al. 2012).

There are currently many technological, economic and logistical challenges facing Continuous Auditing. Some examples include unclear benefits, high implementation costs, few industry standards, limited customer demand, security concerns, unclear

benefits and difficulties with data capture and mapping data between large and disparate data sources (Penler 2006). Like all information system projects, Continuous Auditing systems must balance innovation with efficiency, perpetually reconcile changing and often conflicting user needs, and make difficult technology choices in a constantly evolving landscape, which leads to unanticipated needs for new employee skills, user training, the re-allocation of personnel and resources and the need to retire or integrate with dated technologies (Patten 2009). Most large Information Systems projects have material cost overruns or schedule overruns. Moreover, roughly 17% of large Information Systems projects go so badly that they threaten the existence of the entire company (Bloch 2012). The following subsections explore the challenges that have been described in the Continuous Auditing literature.

3.6.1 Cost

In September 2008, the Economist asked 446 senior executives about their views on the drawbacks of investing in standardizing/automating their financial processes (Fedorowicz 2008). The number one drawback was the high level of investment required, which 48% of the respondents gave as their answer. It was twice as much as the number two answer, difficulty of modeling complex financial processes. Consequently, it is clear that the cost of implementing a Continuous Auditing system is a formidable obstacle. One possible approach to overcoming this cost objection is to phase the system in over time. In the early phases of system development, the system implementer focuses on building the high-value components and phases in the other lower value components over time. While this approach does not directly lower the total cost of ownership, it does lower the initial upfront costs and gives the user the high-value components first.

Another approach to overcoming cost objections is to highlight the cost of doing nothing. As Subsection 3.4.1 points out, there are tangible and intangible cost savings associated with automating manual processes. Moreover, Gartner suggests that organizations that utilize a piecemeal approach to achieve their compliance initiatives will likely spend ten times more on their compliance projects than an organization that takes a more integrated approach (Brace 2006). Table 3.2 compares the costs of traditional auditing techniques with those of Continuous Auditing. Other things being equal, the cost effectiveness case for Continuous Auditing seems to improve as the organization's scale increases.

Table 3.2 Traditional and Continuous Auditing Cost Comparison

	Traditional Auditing	**Continuous Auditing**
Setup Time Cost	Less	More
Operating Costs	Proportional with sizes of organization. Fairly static year over year.	High initial development costs, but markedly drops after implementation
Cost of Audit Exception	Varies based on exception but after-the-fact detection may lead to collateral cost	Preventative and/or near real-time should minimize collateral costs of audit exception
Cost to Scale Up	Very little economies of scale	High economies of scale. Minimal incremental cost to add more sites and/or controls

3.6.2 Inferior to Human Decision Making

The skeptics' biggest criticism of Continuous Auditing is that it is not possible to fully automate the auditing process. They claim that the audit process requires human judgment and estimation, which can never be fully automated nor done continuously (Krass 2002). They argue that although Continuous Auditing may be able to detect a

possible problem, a human will always be needed to confirm and/or mitigate it. For example, a Continuous Audit process could detect a possible fraudulent credit card transaction; however, a customer service representative would generally need to contact the customer to confirm it.

Even a well-defined process can be difficult to automate. For example, in spite of the fact that regulatory bodies painstakingly define standards and guidelines, and organizations spend significant resources defining their business policies and controls, determining whether a corporation is in compliance with a particular standard or guideline still requires a fair amount of human judgment. To illustrate this point, each year Money magazine sends the financial records of a hypothetical family to approximately 50 tax preparers and asks them to determine how much this family owes in taxes. In 1990, the family's tax bill ranged from $37,715 to $68,912, a difference of 83%. The reason for this variation is that determining income, deductions and an appropriate depreciation schedule is a subjective part of the tax preparer's work. Similarly, organizations face a myriad of vastly more complicated but still ambiguous accounting questions, whose answers can lend themselves to self-serving interpretations (Bazerman, Loewenstein et al. 2002).

The skeptics' basic premise is that some auditing data is simply too ambiguous to fully automate the decision process. Peterson defines a continuum between hard and soft data in a financial context (Peterson 2004). Hard data is almost always recorded numerically (e.g., income statements, balance sheets, etc.). In general, it can be easily interpreted, summarized, and electronically collected, stored and transmitted. Conversely, soft data is generally communicated by language (e.g., opinions, ideas,

rumors, economic projections, etc.). Soft data requires more subjective interpretation than hard data does. While soft data is more costly to produce, store and interpret, Peterson concludes that soft data by its nature could contain more nuanced and potentially useful information.

Expanding on the hard to soft data continuum (Woodroof and Searcy 2001) define an audit data taxonomy that has three categories: (1) Routine Hard Data: audit data that is clearly definable and easily interpreted and measured, (2) Non-routine Hard Data: Audit data that requires information from other sources to be interpretable, (3) Soft Data (i.e., data with a high degree of subjectivity that requires some assumptions and judgment to interpret). Consequently, routine hard data is the easiest to audit and soft data is the hardest to audit.

Continuous Auditing systems can easily audit routine hard data (e.g., does a user entering transactions into the general ledger system have the proper authority to make this type of transaction, have any unauthorized changes been made to key system tables, and are the calculations in the system performed correctly?). At the other end of the spectrum, auditing soft data would likely require the application to use some form of artificial intelligence techniques.

(Simon 1966) claimed back in the 1960's that machines will be capable, within twenty years, of doing any work a human can do. Although artificial intelligence, thus far, has not lived up to these early expectations, in some small well-defined areas it has been able to equal or outperform humans. For example, the artificial intelligence program deep blue has beaten the world's best grandmasters at chess (Loeb 2006). Watson has beat some of the world's best players at Jeopardy (Markoff 2011). Also,

artificial intelligence is replacing skilled practitioners in fields such as law, medicine and aviation (Dewhurst and Willmott 2014). For example, pilots are flying airplanes less and less because they rely more and more on flight automation that has become reliable and efficient, and eliminates the risk of pilot fatigue. However, these automation controls are not foolproof. Some have believe that they played a role in the 2009 Air France crash that killed 228 passengers, which paints a cautionary tale of the perils of designing an automated control system that does not cleanly mesh with our innate human understanding or the world (Wise 2011).

Recent advances in deep learning techniques have led to renewed enthusiasm among researchers that automating some types of human tasks is becoming increasingly plausible in the foreseeable future (Markoff 2012). Some have predicted that Artificial Intelligence will reach human level by 2029 (Devlin 2015). Others have even heralded the next wave of artificial intelligence that could result in a paradigm shift for senior executives (McKinsey 2014). However, it still remains unclear whether similar technology could be used to create superior artificially intelligent auditors.

One formidable obstacle is that complex business decisions may require multi-criteria decision-making, which refers to decisions that have conflicting criteria and require implicit or explicit tradeoffs between competing objectives. These types of decisions generally require the aggregation of input from various disparate parties that very well may have sharply different views, responsibilities and objectives. Benjamin Franklin suggested a process to make a multi-criteria decision: simplifying the decision process by simultaneously removing even swaps from a decision's pros and cons column until the best decision becomes apparent (Hammond, Keeney et al. 2001). Etzioni

champions a humbled decision making model, which has been used by physicians for centuries (Etzioni 2001). This model requires an understanding of organizational goals and policies, and advocates small, nonbinding and experimental decisions based on in-depth examination of a focused subset of facts and possible decisions.

A contemporary solution to the multi-criteria decision-making problem, which was suggested by emergency management research, is to combine a real-time decision support system that provides consistent and comprehensive information with a structured approach that allows experts to model decisions and their effects (Roethlisberger 1939). Turoff defines a theoretical emergency management system that combines decision support templates, Continuous Auditing of a predefined set of emergency preparedness controls and Continuous Auditing of the decision process to establish oversight and accountability (Turoff 2004).

3.6.3 Automation Issues

Software developers have relied on automated testing tools to validate the correctness of a software project. Continuous integration, which is a software engineering practice that advocates implementing continuous processes as a means for quality control, has been pushing the boundaries of automation in software development. Continuous integration recommends automating the build and unit testing processes such that they are automatically executed every time a software module is changed. One of the advantages of continuous integration is software bugs emerge early in the development process. However, the disadvantages are increased set up time, and the cost of developing an adequate unit test suite and purchasing the requisite hardware and software (Roebuck 2011).

Continuous Auditing, which aspires to a much grander scale of automation, will likely face similar, if not materially more difficult, automation challenges. The cost of developing and maintaining automated tests have been higher than expected (Ramler and Wolfmaier 2006). There is the upfront cost of determining which automation tool to buy and learning how to use it. Then, there is the ongoing cost of developing, executing and maintaining the automated tests. Developing a suite of automated tests generally require costly, highly specialized and technically competent resources that understand the testing tool as well as the underlying domain space.

Even highly automated tests still require a fair amount of human supervision. For example, each time the test suite is executed the results need to be carefully reviewed to determine the false positives from the real issues. Moreover, automated tests may also require human intervention to fix broken tests and resolve technical snafus such as memory problems, network glitches and, perhaps, even bugs with the testing tool itself. Changes to the underlying information technology systems or the audit objectives are likely to necessitate a corresponding change in the tests suite as well.

Automated tests tend to be rigid. In general, automated tests have difficulty coping with rapidly changing environments or environments where the underlying domain space is not well understood. In these environments, automated testing may not even be a viable option (Bach 1999). Berner and Weber concludes that automated testing cannot fully replace manual testing (Berner, Weber et al. 2005). They also point out that the capability to run automated test cases diminishes, if they are not used. In conclusion, automated testing has been effective in certain domains; however, it has some systemic issues that have limited its overall effectiveness. It is highly probable that those seeking

to implement a Continuous Auditing system will wrestle with the same type of automation issues, albeit on a grander scale, as what test engineers encountered when they build automated test scripts for Information Systems.

Having to regularly update and improve a Continuous Auditing system is probably inevitable except for the extremely rare environment that never changes and is totally free from the surprises caused by human missteps, competing organizations and natural events. Therefore, model and test updates probably should be viewed as a routine exercise that if not done regularly will cause the accuracy of the system to steadily decay. Practically speaking, there probably should be a periodic recheck of automated predictive models at least once a year to verify the fidelity of their forecasts.

Finally, Exception Reporting, which was first proposed by the father of scientific management (Taylor 1911), highlights the inherent problem of defining exactly what "exceptions" to a business process are (Gorr 2009). The number of possible exceptions is nearly infinite. Even with large-scale data mining, there is always the possibility that an abnormal finding has not yet been captured in an organizational database, which greatly exasperates the modeling process.

3.6.4 System Performance

Adding Continuous Auditing controls and/or data extraction methods (see Subsection 4.2.3) to an existing IT system may negatively impact system performance. Hoxmeier concludes that user satisfaction with an IT system decreases as response time increases (Hoxmeier 2000). In the best case, lengthy system response times will lower user productivity and, in the worst case, render the system unusable.

(Murthy 2004) examined the system performance implications of adding three types of controls (calculations, database lookups, and aggregate function controls) to an e-commerce application. Calculation controls make comparisons between the current transaction and data retrieved from a single database lookup. Lookup controls are similar to calculation controls but require data from multiple tables. Aggregate function controls compare transaction values to the average, sum, maximum and/or minimum of a particular field. For example, one aggregate control compares the customer's current transaction amount to the customer's average historical amount. Murthy concludes that calculation controls could be accommodated, regardless of system load. Lookup controls had a detrimental effect on system performance only during peak periods. Aggregate function controls had a dramatic negative impact on system performance irrespective of the system load.

However, as information technology systems continue to become more powerful, the system performance concerns over Continuous Auditing may diminish in materiality. Today's highly scalable and distributed computing grids can quickly process a tremendous amount of data. For example in 2011, Facebook processed over 30 billion pieces of content each month (Manyika, Chui et al. 2011).

3.6.5 Formalizing Business Processes

A September, 2008 Economist study asked 446 senior executives their opinions on how to improve financial processes. In response to the question "What is the biggest problem with current financial processes?" the top three issues were: (1) Too many manual processes (2) Complex procedures which are difficult to model or automate (3) Inconsistent methodologies around the organization (Fedorowicz 2008).

Continuous Auditing strives to mitigate these issues through the formalization of business processes, controls and audit exceptions. Knowledge Management, which has been extensively researched (Malone, Crowston et al. 2003), attempts to formalize, organize, describe and leverage the intellectual capital that has been embedded in business process routines and machinery (Davenport and Prusak 2000) and could serve as a basis for a Continuous Auditing system. In general, formalization promotes precision and consistency, improves confidence in audit results and reduces long run audit costs. Once a business process has been formalized, it can usually be automated. Unfortunately, many humans resist formal thinking, formalization can be very laborious and costly and some complex judgments are not amenable to formalization (Alles, Brennan et al. 2006). Consequently, formalizing manual audit procedures to facilitate automation is much more difficult than might have been anticipated (Alles, Brennan et al. 2006).

Conventional audit programs may not be designed for automation because formalization and judgmental procedures are often intermixed. In order to optimally automate the audit process, the whole process may need to be reengineered. Wherever practical, continuous automated procedures should be relied on, and manual methods and informal judgmental procedures should be eliminated (Alles 2008).

3.6.6 Information Overload

Continuous Auditing systems could increase the quantity of data available for analysis, which could cause information overload. Information overload occurs when the volume of information supplied in a given unit of time exceeds the limited human information processing capacity, which tends to lead to confused and dysfunctional behavior (Jacoby,

Speller et al. 1974). Chewning and Harrell demonstrated that an overload of accounting data leads to decreased decision quality in accounting students (Chewning and Harrell 1990).

The Information Systems literature explores possible solutions to the information overload problem: installing voting structures to evaluate information (Hiltz and Turoff 1985), using decision support systems (Cook 1993) or intelligent agents to limit alternatives (Edmunds and Morris 2000), providing flexible information organization, filtering and routing options (Hiltz and Turoff 1985), utilizing data visualization tools (Chan 2001), creating a measurement system for information quality (Denton 2001), compressing, aggregating and categorizing data (Grise and Gallupe 1999), defining decision models (Chewning and Harrell 1990) or exception reporting (Ackoff 1967), and using search procedures (Olsen, Sochats et al. 1998).

Siemens designed their Continuous Auditing system to prevent information overload by implementing an exception-based approach built around intelligent alarms. When critical exceptions occur, the system automatically generates alarms, which are emailed to all relevant parties. To prevent alarm floods, which occur when the same alarm is repeatedly sounded, from hampering the ability to react to the underlying problems and, in the worst case, having the alarm ignored altogether, a hierarchical alarm structure was implemented where each node has an enabled/disabled flag. Disabling the node prevents its children's alarms from sounding, thereby preventing alarm floods. Moreover, the system intelligently monitors alarms, waits a predefined amount of time before re-sounding an alarm and initiates escalation procedures if an alarm is not resolved within a given timeframe (Alles, Brennan et al. 2006).

CHAPTER 4

INFORMATION SYSTEMS

4.1 Architecture

This chapter surveys the enabling Information System technologies for Continuous Auditing and Monitoring systems. At the highest level all Information Systems require a software architecture. A software architecture is defined as "the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution" (ANSI/IEEE 2000, p. 3). Although much has been written about empirical and theoretical Continuous Auditing architectures, there is still disagreement on the optimal system architecture. Gartner defines the critical capabilities of the Continuous Auditing system as: Detection and Preventing of Conflicting Privileges (i.e., ensuring that an employee does not have system access that violates the organization's **S**egregation **o**f **D**uty (SOD) policy), transaction monitoring (i.e., periodically run predefined analytics to identify control exceptions), auditor and management workflows (i.e., supports tracking and remediation audit exceptions) and cross-platform integration (i.e., the ability to extract data and track business processes across multiple ERP systems and home-grown financial application) (Proctor and Caldwell 2010).

(Alles, Kogan et al. 2004) generically describe the seven components of a Continuous Auditing system:

1. A layer of software (aimed at process control and monitoring) on top of the most critical corporate software systems.
2. An instantiation of the control and monitoring process aimed at business process assurance by both internal and external assurors.

3. A constant stream of measurements (metrics) engineered out of key processes.
4. A sophisticated dynamic set of standards (models) to compare with the metrics.
5. A set of dynamic exception metrics to determine when an alarm is to be issued, and its degree of importance.
6. An analytic layer to perform additional analysis related to several corporate functions (auditing, fraud evaluation, accounting rule compliance, estimate review).
7. A new level of statutory reporting that may include reports to governmental agencies.

One possible extension of this approach is to incorporate periodic revalidation of the model's efficacy on a regular basis. This review should be consistent with the rate of external changes that affect the organization's operation.

(Warren 2005) describes a web enabled software architecture that receives a continuous feed of data from a variety of enterprise systems and performs Continuous Auditing, audits and control checks on this data. Ye posits that a **S**ervice-**O**riented **A**rchitecture (SOA) Continuous Auditing architecture would provide faster business value, rapid response capabilities and reuse (Huanzhuo Ye 2008). Woodroof and Searcy adds the concept of continually combining data from multiple disparate organizations (Woodroof and Searcy 2001). The auditor's website aggregates information from three disparate entities (the client, its supplier, and an independent valuation engine) to generate Continuous Auditing reports. Alles and Brennan adds the notion that formalizable procedures should be separated from non-formalizable ones, where the formalizable controls are executed with high frequency (perhaps continuously), while non-formalizable ones should continue to be done manually and periodically (Alles, Brennan et al. 2006).

4.2 Information Management

(Marchand, Kettinger et al. 2000) defines Information management capability as the ability to provide data and information to users with the appropriate level of accuracy, timeliness, reliability, security and confidentiality. An effective Continuous Auditing system would require strong information management and governance practices (Caldwell, Wheatman et al. 2009). Although today's organizations are not entirely paperless, technologies such as **E**lectronic **D**ata **I**nterchange (EDI), **E**lectronic **C**ommerce (EC), and **E**lectronic **F**unds **T**ransfer (EFT) are greatly increasing the number of digitized audit trails while simultaneously reducing the number of paper based ones. Redgrave estimates that 93% of information created today is in a digital form, 70% of an organization's records are stored electronically and 30% of electronically stored information is never printed (Redgrave 2005). The trend towards digitizing an organization's audit trails is a necessary prerequisite to Continuous Auditing, because at the core of any Continuous Auditing system is electronically stored data. If this electronic data can be properly aggregated and structured, it could likely be used to satisfy multiple governance and business reporting needs (Hannon 2005).

4.2.1 Big Data

The global economy is generating a tremendous volume of transactional data, which includes trillions of bytes of information about customers, suppliers and business processes. If this data can be appropriately harvested, it could be transformed into a major corporate asset. For example, GE turned the 50 million data points generated from the ten million sensors embedded in the wide array of products it has sold into an estimated annual $1 billion predictive maintenance revenue stream (Clancy 2014).

Big Data seeks to analyze and create value from a massive data set. However, big data has some notable limitations: It increases the number of spurious statistically significant correlations, has difficulty modeling the strength of social relationships and understanding the contextual decision-making framework. Moreover, Big Data can be riddled with some latent predispositions and perceptual biases imbued by its creator and will be of only marginal usefulness in black swan events (i.e., novel situations where no pre-existing representative data exists) (Brooks 2013). Finally in the audit context, exhaustingly analyzing Big Data sets could generate a prohibitive number of audit exceptions, which would be difficult to manually review and process on either timely or cost effective basis.

Two of the objectives of Big Data research are similar to the goals of Continuous Audit: 1) Creating Organizational Transparency by making the data more understandable to relevant stakeholders in a timely manner. 2) Replacing/supporting human decision making with automated algorithms that could lead to improved decision making, minimized operational risks, and potentially lead to new and valuable insights (Manyika, Chui et al. 2011).

4.2.1 Database Management Systems

A Continuous Auditing system will almost certainly require some form of Database Management System (e.g., SQLServer, Oracle, DB2, etc.). Alles and Brennan propose that a large relational database application is an appropriate tool for an Audit Data Repository (Alles, Brennan et al. 2006). Most modern database systems have SQL-based querying capabilities that allow selecting, aggregating and filtering the data stored in the database. Moreover, these database management systems generally have **E**xtract

Transform and **L**oad (ETL), Data Warehouse, Data Mining and Predictive Modeling. Warren suggested that these capabilities could be key components of a Continuous Auditing System (Warren 2003). ETL tools help extract data from other IT systems, transform it into the current database model and load the data into a database. A Data Warehouse organizes information stored in the database to facilitate end-user reporting and analytics. Data Mining is a systematic process for extracting patterns from data (e.g., fraudulent transactions). Predictive modeling creates a model based on the underlying data that is used to predict future results, activity or behavior.

4.2.2 Data Sources

Few organizations have a completely homogeneous system environment. In an (ACL 2006) survey of 858 audit executives in organizations with annual revenues in excess of $100 million, over half of the respondents (58%) felt that fragmented and incomplete data was an extremely important issue facing their organization; 28% felt it was important; 11% indicated it was slightly important; and only 3% of respondents felt that this was not a key challenge in their organization at this time.

Typically, organizations have a complex IT environment, which could be composed of a hodgepodge of **E**nterprise **R**esource **P**lanning (ERP) systems or perhaps multiple instances of the same ERP, mainframe systems, off the shelf applications and legacy systems, all of which may contain valuable data to the auditor (ACL 2006). Some of the Continuous Auditing literature mentions the concept of an Audit Data Repository, which ideally contains all the data needed for an audit and organizes it from an audit perspective.

Practically speaking, the economics of saving, organizing and managing all this data could be prohibitively expensive. Moreover, there could be political problems that stem from providing auditors unfettered access to this information. Alles and Brennan posits the greatest opportunity for reducing the volume of data stored in an Audit Data Repository is adjusting the retention requirements such that data is only retained if it generates exceptions that require follow-up. Since all other data is purged, the total data stored, and potential security and confidentiality risks are reduced (Alles, Brennan et al. 2006).

A couple of papers have described Continuous Auditing systems that were based on ERP systems. Kuhn described a hypothetical Continuous Auditing system built on top of an ERP system similar to the one used by WorldCom (Kuhn 2006). Alles and Brennan describe Siemens' Continuous Auditing system built on top of their SAP systems (Alles, Brennan et al. 2006).

(Rezaee 2002) proposes a data mart that does not necessarily require an ERP system. Data marts collect and transform data from various business units. The data are transformed and stored in an audit data server for easy access, analysis, and reporting. An integrated audit data mart must have the following characteristics:

- Integrated query, analysis, and reporting through a unified user interface,
- Easy-to-use yet powerful enough for the most sophisticated analytical users,
- Capacity to easily export queries to common spreadsheets and database systems,
- A query engine capable of retrieving and processing large volumes of data,
- Data aggregation and multidimensional database capability,
- Advanced statistical modeling and data exploration capabilities,
- Data visualization for data mining exploration,

- The ability to drill down into different degrees of data aggregation.

The Table 4.1 summarizes the difference between ERP and Audit Warehouse Continuous Auditing solutions.

Table 4.1 ERP versus Audit Warehouse

	ERP	**Audit Warehouse**
Data Storage	Optimized for transactional processing	Optimized for Audit Analysis
Potential Scope of Data	ERP System only	All digital systems including multiple ERPs
Require ETL	No – All analysis is done off of ERP's internal databases	Yes – Data must be continually aggregated from multiple systems
Data Latency Issues	Generally no. All analysis is performed on the ERP's internal data stores	Yes – Data could become stale between refreshes

Both approaches are used in commercial applications. Data 2 Knowledge is an example of a data mart without an ERP (D2K 2005). Data 2 Knowledge transforms the contents of an unlimited number of log files into a single structure database. Approva's Bizrights is an example of a Continuous Auditing implementation that requires an ERP solution, such as Oracle, PeopleSoft, SAP or J.D. Edwards ERP. Bizrights continually scans these ERP's databases for potential audit exceptions such as duplicate payments, nonstandard payment terms, cash payments to vendors, invoices without purchase orders, etc. (Approva 2009).

(Murthy and Groomer 2004) theorized how extensible markup language (XML) and Web services could be utilized to create a **C**ontinuous **A**uditing **W**eb **S**ervice (CAWS). CAWS could be used by an external auditor to extract data from an auditee's IT system(s) on demand. This data could be analyzed and potentially aggregated with

data from other companies in the supply chain to produce a real-time assurance report for other counterparties (i.e., investors, analysts, financial institutions, etc.). They suggest that **B**usiness **P**rocess **E**xecution **L**anguage (BPEL) or e**X**tensible **B**usiness **R**eporting **L**anguage (XBRL) standards are a plausible foundation for CAWS. In one example, they depicted an XBRL GL implementation that used a Data Hub (i.e., Data Mart).

(Vasarhelyi 2004) suggests transaction tagging, which tracks transactions as they flow between applications, would be a useful data point for a Continuous Auditing system. The transaction tag for the data would include the source, description and validation information that would enable the Continuous Auditing system to monitor and evaluate data accuracy and integrity.

4.2.3 Data Extraction

The Continuous Auditing literature identifies two possible approaches for extracting the requisite data from enterprise systems: the **E**mbedded **A**udit **M**odule (EAM) and **M**onitoring and **C**ontrol **L**ayer (MCL). Embedded audit modules capture information of audit significance on a continuous basis (Groomer and Murthy 1989).

EAMs are generally application level code that is specifically written to identify and continually write to a log file certain key business events. This log file is subsequently reviewed by auditors. For example, EAM could be written to identify all purchase orders that exceed a certain predefined threshold. Once a purchase order that exceeds a threshold is entered into the system being monitored an exception record would immediately appear on the audit log. This file would be used by auditors to manually review the most risky purchases. Since only data for key business events are extracted,

the data are extracted with minimal strain on the underlying systems in terms of processing time, disk IO and network bandwidth.

Although EAM can reduce the strain of data extraction, extracting large volumes of data could still degrade the performance of the production system. Using EAM ghosting, where the entire production system including data and system settings is cloned onto separate hardware could totally alleviate the data extraction burden from the production system. The "ghost" production system would have EAM data extraction enabled and the real production environment would not. Leveraging techniques similar to disaster recovery and fail over solutions, EAM ghosting could be implemented by either having a replica of the production hardware, (e.g., perhaps by reusing the quality assurance testing environment) or through virtualization (Kuhn Jr and Sutton 2010). At predefined intervals, the data from the real production system would be copy to the ghost production system.

(Debreceny, Gray et al. 2005) studied EAM within the content ERP systems. Kuhn extends this research to SAP's ABAP programming language that enables the creation of custom audit rules that can evaluate SAP transactions in real-time, and generate reports and alarms when transactions violate these audit rules (Kuhn Jr and Sutton 2010).

The MCL is generally implemented at the database level and periodically extracts all relevant data from the ERP database into a monitoring and control layer. The MCL data structure is optimized to facilitate the tasks that auditors normally perform (Vasarhelyi 2004). For example, an auditor could use the MCL layer to drill down to the individual transactions and perform aggregate analysis at any level. For additional

security, the MCL could be stored off-site, which would make it highly resistant to modification and tampering, even from internal IT employees with the highest system-level access. (Coderre 2005) identifies three less automated data extraction methods:

1. Run copies of standard reports and save reports in electronic format for further analysis.
2. Run queries or generate reports with a report writer.
3. Obtain physical and logical access to the client system and sign on as a user with read-only access.

The Table 4.2 summarizes the main differences between EAM and MCL data extraction methods.

Table 4.2 Summary of EAM and MCL Data Extraction

	EAM	**MCL**
Extract Frequency	Continuously	Periodically
Extraction Point	Application Level	Database Level
Data Extracted	Exception Data	All Data
Primary Advantage	Data extraction requires minimal system resources	Data is less vulnerable to manipulation by enterprise personnel who have super-user privileges especially when it is stored in a off-site database
Primary Disadvantage	Audit Modules are tightly coupled with enterprise system, so creating Audit Modules requires detailed understanding of the enterprise system.	Requires frequent and system intensive data extracts.

4.2.4 Information Security

Like all of an organization's Information Systems, a Continuous Auditing system should conform to the organization's information security policy. There have been numerous standards published on information security policies (Höne and Eloff 2002). Loch and Carr states the primary objective of information security is to protect Information

Systems and its data from unauthorized access, use, disclosure, disruption, modification or destruction in order to ensure the information system's integrity, confidentiality and availability (Loch, Carr et al. 1992).

Information security has been mentioned in Continuous Auditing literature. Woodroof and Searcy identifies four data security attributes for the Continuous Auditing system:

1. Authorization: Information is limited to only authorized users, which can be accomplished through passwords and/or biometric devices.
2. Confidentiality: using various encryption techniques to ensure the privacy of transmitted information.
3. Integrity: the ability to detect when the underlying data has been tampered with.
4. Authentication: the ability to determine the original source of the data (Woodroof and Searcy 2001).

For a Continuous Auditing system, (Alles 2008) adds the following security concerns:

- Location of the Continuous Auditing hardware (i.e., the corporation's premises or the auditor's premises),
- Physical access security,
- Logical access security,
- Super-user privileges,
- IT personnel access to the Continuous Auditing system's internal security settings.

However, Information security topics such as business continuity, disaster recovery, cryptography and availability have received less attention in the Continuous Auditing literature.

Continuous Auditing has been used to ensure that an organization's key Information Systems comply with its security policy. Harrison states the two main benefits of continuously auditing an organization's information technology controls are

timely notification of threatening conditions, and avoiding the high cost and low effectiveness task of manually sampling security logs (Harrison 2005). Siemens uses Continuous Auditing techniques to monitor SAP's password and user access policies (Alles, Brennan et al. 2006). Therefore, a Continuous Auditing system could be designed to monitor its own compliance with the organization's security policies.

4.3 Analytical Methods

Continuous Auditing seeks to improve the audit process by continually applying predefined analytical methods to impartially analyze vast amounts of data (e.g., financial transactions, application configuration settings and customer data). Analytical methods can consider nearly an unlimited number of factors, provide deep insights and scale to meet the needs of even the largest company. However, these methods can also be perilously misled by bad data and false assumptions (Redman 2014).

These analytic methods are designed to identify control exceptions (Caldwell 2009). There is a long lineage of research that suggests just the act of continually monitoring a process tends to improve its overall quality. The Hawthorne effect, where subjects improve an aspect of their behavior that is being experimentally measured simply in response to being studied and not in response to an experimental manipulation, was first documented in (Roethlisberger 1939). More recently, various Total Quality Management processes have used continual analysis as a way to improve business process. For example, Six Sigma has a five-step process:

1. Define the process and high-level objectives,
2. Measure key aspects of the current process,
3. Analyze the data to determine cause-and-effect relationships,

4. Determine what the key relationships are,
5. Optimize the process based upon data analysis techniques (Pyzdek 2009).

Using feedback to improve analytical methods is a powerful technique as evidenced by the steady improvement in models that predict weather. For example, the average error in maximum temperature prediction was six degrees Fahrenheit in the 1970s and just 4 degrees in 2010 (Rosenzweig 2014).

As the time to complete an audit shrinks, the necessity of relying on fully automated programmatic solutions to identify audit exceptions increases. There have been many research articles that have suggested various analytical methods that could be used in a Continuous Auditing system to identify audit exceptions. These analytical methods all share the following properties: observing events in real or near real-time, generating alarms when exceptions occur and performing repeat tests quickly, continually and with low variable costs (Vasarhelyi 2004). The following subsections describe the most promising analytical methods in more detail.

4.3.1 Belief Functions

A belief function allows the combination of evidence from several different sources to calculate the degree of belief that utilizes all the available evidence. There have been several journal articles speculating that belief functions would be useful in a Continuous Audit system. For example, (Srivastava and Shafer 1992) used a belief function framework to calculate the total plausibility of a material misstatement at the financial statement, account and audit objective levels.

4.3.2 Continuity Equations

Continuity equations use statistical models to capture relationships between various business processes. They can be used to create expectation models for how data moves through a business process. Continuity equations are developed using statistical methods (e.g., Linear Regression Modeling, Simultaneous Equation Modeling, Multivariate Time Series Modeling, Vector Autoregressive Model, Subset-VAR or Bayesian-VAR).

There is a three-step process to modeling a business process with continuity equations:

1. Choose a business process to model (e.g., purchasing, payments, inventory etc.).
2. Define metrics to represent each process: (e.g., dollar amount of purchase orders, quantity of items received, or number of payment vouchers processed).
3. Choose the levels of aggregation of metrics (By time: hourly, daily, weekly; by business unit; by customer or vendor; by type of products or services; etc.).

The model's prediction accuracy can be compared using statistical methods such as Mean Absolute Percentage Error, Mean Absolute Error or Symmetric Mean Absolute Percent Error.

4.3.3 Expert Systems

Expert Systems are an artificial intelligence technique that encapsulates the knowledge of one or more human experts in a series of rules. Typically, expert systems are well suited for static and narrowly defined problem sets that lend themselves to analytical solutions. Within an auditing context, (Coderre 2009) asserts that expert systems would be well-suited to provide consistency across audits that are performed at different locations or clients.

(Davis, Massey et al. 1997) combined the deductive power of a rule-based system with the inductive power of a neural net to assess the audit risk embedded in an organization's control structure. Essentially, Davis calculated the probability that an entity's control structure would fail to prevent or detect significant financial misstatements. Siegel and Strawser use rough set theory, which is an analytical method that generates a compact set of rules from an empirical set of multivariate data, to develop decision rules for evaluating internal controls (Siegel, Strawser et al. 1998). These decision rules were based on expert assessment of control risk after considering certain control procedures surrounding the decision. The paper concludes that these rules allowed non-experts to make decisions comparable to those made by firm-wide experts. Similarly, (Greco, Matarazzo et al. 1998) applied rough set theory to evaluate bankruptcy risks.

4.3.4 Fuzzy Sets

Fuzzy logic is an analytical method that linguistically describes a process using a combination of fuzzy sets and rules. Unlike traditional logic theory, which has only a binary true-false set, fuzzy logic has a degree of membership construct that could assume any value from between zero to one inclusive. Dhar and Stein suggests that fuzzy logic is an intuitive and flexible way to describe the behaviors of very complex systems. Fuzzy logic has been mentioned in the Continuous Auditing literature (Dhar and Stein 1997). For example, (Deshmukh, Nassiripor et al. 1998) illustrates how lenders could improve their decision-making by using fuzzy sets to assess short-term liquidity risks. The paper concludes that this model is superior to traditional measures of liquidity. Deshmukh and

Romine built a fuzzy logic model to determine whether an accounting firm should either initiate or continue a relationship with a client (Deshmukh, Romine et al. 1998).

4.3.5 Neural Net

Neural Nets are a predictive modeling technique that simulates the workings of the human mind. Coakley used a neural net to detect material errors in monthly financial ratios (Coakley 1995). Two separate journal articles used neural nets to detect concerns in financial statements' ratios and values (Hian Chye and Sen Suan 1999) (Etheridge, Sriram et al. 2000). Koskivaara used neural nets to recognize patterns in the monthly balances of financial accounts (Koskivaara 2000).

Moreover, (Ramamoorti, Jr et al. 1999) used 26 quantitative and 19 qualitative risk factors as input into a neural net to assess internal auditing risk at the University of Illinois. The quantitative data were extracted from the Financial and Administration Systems. The qualitative risk factors were ranked by the audit staff using a Delphi, which was used to train the neural nets. Ramamoorti concludes that internal auditors could benefit from using neural nets.

In general, neural nets tend to perform well when, data samples and the range of values to be analyzed are large, the data does not conform to strict distributional properties and the underlying associations among the data are ill defined. However, neural nets are difficult to explain conceptually (i.e., how and why they arrived at the conclusion they did) and do not readily allow the calculation of statistical significance for the model's variables (Calderon and Cheh 2002).

4.3.6 Regression-based

Regression analysis is a predictive modeling technique based upon statistical methods. Knechel compared seven regression based analytical review procedures on monthly account balances (Knechel 1988). When these rules identified months with inordinately high variance, the auditor would randomly sample and manually review the transactions within these periods. Knechel concluded that allowing regression based analytical review procedures to guide the auditor's transaction review was an efficient approach, because even in the worst-case, most analytical review procedures in spite of their smaller samples sizes still had only a small increase in detection risk versus traditional sampling techniques.

(Vasarhelyi 2004) recommends using time series/cross-sectional analysis to model the normal behavior so that audit exceptions can be detected. In general, regression based statistical techniques are easily explainable and their variables' significance can be easily calculated. However, regression based statistical techniques force the underlying data into a preselected distribution (e.g., normal, logarithmic, etc.), which may not fit the underlining data distribution.

4.3.7 Qualitative

Soft information may need to be incorporated into a Continuous Auditing system. In this context, soft information is defined as management estimates and/or judgments (e.g., calculating and allowance for doubtful accounts or determining a new organizational risk are examples of auditing tasks that require a fair amount of human judgment) (Warren 2002). In order to incorporate soft information into a Continuous Auditing system it must be electronically captured. Since this process requires human input, strictly

speaking it could not occur continuously, but potentially could be a source of valuable information that would be difficult to obtain using other analytical methods.

One qualitative method that can be used to digitize human judgment is an electronic questionnaire. An electronic questionnaire can range from a simple true-false questionnaire form to a complex interactive form dynamically leading the user through relative questions based on previous answers (Coderre 2009). On an electronic questionnaire, the question types could be nominal (e.g., yes/no), ordinal (e.g., Strongly Agree (5) Agree (4) Neither Agree or Disagree (3) Disagree (2) Agree (1) Strongly Agree), interval (e.g., a scale from 1 to 100), open ended, or any combination of the aforementioned.

Another electronic qualitative approach is the Delphi method, which is an interactive forecasting model that would rely on a panel of independent experts either inside or outside the organization. These experts would answer preselected questions in multiple rounds. After each round, a facilitator provides an anonymous summary of the expert's forecast from the previous round as well as the reasons they provided for their answers. In the next round, the panel could revise their answers based upon input from the previous round. This process continues until a predefined stop criterion (e.g., achievement of consensus, stability of the round's results, etc.) is reached (Linstone 1975). A Delphi study was used to predict the answers to some of the open questions in Continuous Auditing. The Delphi predicted that by 2020, 68% of the external audits and 78% of the internal audits will be automated (Vasarhelyi, Lombardi et al. 2010).

The Delphi process could be used to build collaborative models that aggregate the collective wisdom of multiple experts, and help detect and mitigate risks. Linstone and Turoff review of the current status of the Delphi method makes two important points:

1. Collaborative Model Building is currently a major Delphi research objective.
2. While the Web has ushered in the "age of participation", we need new types of software to get us to the "age of collaboration." (Linstone and Turoff 2011)

Bañuls and Turoff explain how a Delphi process, Cross Impact Analysis and Interpretive Structure Modeling could be used to produce collaborative models (Bañuls and Turoff 2011). They created dynamic scenarios with influence relationships such that modifying any event's probability shows its impact to all the other events. Bañuls, Turoff explore collaborative modeling within the context of a dirty bomb exploding in an urban area (Bañuls, Turoff et al. 2013). It demonstrates that a group of professionals could build collaborative models without any programming skills. For other types of risks, it may be possible to use this same technique to create working models that were informed by a cross-functional array of domain experts.

4.4 Alarms

Alarms are an early warning system that let stakeholders know when issues or opportunities arise that requires action. Early warning systems must identify the key information to be monitored, the criteria necessary to generate the alarm, and the recipient, frequency and medium of the alarm. To maximize an alarm's utility, alarms should be relevant, information rich and not overly repetitive.

Several Continuous Auditing articles describe the need for audit alarms to sound when an audit exception occurs. Vasarhelyi and Halper first suggested the alarm concept in his continuous process auditing system developed for AT&T Bell laboratories internal audit department. In this implementation, when the predefined system rules were violated, alarms were triggered, which were intended to call attention to this system anomaly. There were four types of alarms: Type 1 alarms were minor alarms that dealt with the functioning of the audit system; Type 2 alarms were low-level operational alarms designed for operating management; Type 3 alarms were higher-level exceptions that were sent directly to the auditor; and Type 4 alarms warned auditors and top management of a serious crisis (Vasarhelyi and Halper 1991).

In a debt covenants system, (Woodroof and Searcy 2001) used alarms sent over the Internet to notify the lender when the borrower is potentially not in compliance with its debt covenant agreement. Alles and Brennan used a hierarchical role-based approach to determine an alarm's destination. In their implementation, the alarm was always sent to the auditor. The alarm could also optionally be sent to the responsible enterprise personnel and/or manager as well as other relevant parties. If the alarm was not resolved in a timely manner, it was propagated up the organization's hierarchy. In order to prevent alarm floods, which is when the same alarm is repeatedly sounded, every alarm in the hierarchy had an enable/disable flag. If the flag is disabled at a point in the hierarchy, the alarms for all of the nodes below it are also disabled (Alles, Brennan et al. 2006).

Other related research supports the hypothesis that alarms will be a critical part of a Continuous Auditing system. For example, there is a stream of research on highly reliable organizations, which avoid catastrophes in spite of the risky and complex

environment that they operate in. Highly reliable organizations also tend to share five characteristics, two of which could be fostered by an effective alarm system: preoccupation with failure and sensitivity to operations. These organizations tend to encourage reporting of errors so that they can learn from them. They try to identify and respond to errors in the earliest stage, where there is often only a vague sign of trouble.

Sensitivity to operations describes a highly reliable organizations' constant concern with unexpected variability in their business processes. Unexpected variability can stem from latent failures in a business process's controls. If latent failures are left uncorrected, they tend to continue and become more frequent and severe as time progresses. Many times, they are only detected after a material breakdown has occurred, but this need not be the case. Highly reliable organizations tend to continually and carefully monitor their normal operations to detect the onset of latent failures. Identifying and addressing latent failures in the earliest stages prevents them from deteriorating to the point of manifesting into catastrophic failures (Weick 2001).

4.5 Black Box Log

A black box audit log is a confidential log of all of an organization's germane audit procedures and other economic events. It creates a permanent and non-updatable record of the most important audit procedures with an audit trail of its own that is kept private and secure. The benefits of a black box audit log are it would allow a tertiary monitor to perform peer review audit on the organization, a clear record of accounting and audit decisions and assist in determining accountability for a financial collapse of an organization. It is designed to enhance the integrity of audit data by enforcing standard

control principles such as adequate record maintenance, separation of duties and proper authorization of audit activities (Alles 2003).

Generally, black box audit logs will rely on a database management system to track the requisite transaction log, supporting documents and revision history of the aforementioned. There are several approaches to making the database management systems non-updatable. At the hardware level, EMC, IBM and NetApps sell off the shelf magnetic, optical and tape drives that are based on **W**rite **O**nce and **R**ead **M**any (WORM) technology (Pavlou 2011). These drives prevent the data from being modified once it is written. However, (Hsu 2004) asserts that worm drives can be tampered with if the drive's metadata is not also protected. They define a fossilization process, which is a holistic process to managing data that ensures that it is trustworthy (i.e., has not been tampered with). The three-step fossilization process is (1) ensure that all the data and associated metadata are reliably stored and protected from modification; (2) ensure that the preserved data can be quickly discovered and retrieved; (3) ensure that the preserve data are delivered in an intact form. They also advanced five principles for implementing the fossilization process:

1. Raise the barrier to attack.
2. Focus on end-to-end trust.
3. Limit what must be trusted.
4. Use simple and well-defined interfaces between trusted and untrusted components.
5. Verify all operations.

There are also software solutions to prevent data tampering: (1) Cryptographic hash, which for an arbitrary block of data calculates an unique digital signature that would change if the underlying data modified (Bakhtiari 1995); (2) Fragile watermarking,

which is a watermark that is readily destroyed when the underlying data is modified (Alomari 2004). These techniques could be applied at the software level to ensure the data has not been tampered with.

Another approach is to make the black box audit logs read-only, encrypted and under the supervision of a third party (Alles 2003). Pavlou suggests that a Cloud Service Provider maybe the ideal location to store the black box audit log (Pavlou 2011). Other things being equal, storing the black box audit log in the cloud would make it more difficult for the employees of the organization that own the data to tamper with it, if only because the exact physical location of the data is likely unknown to the employees of the organization. Also, the Cloud maybe more scalable and distributed than the organization's internal computing environment, which may provide a cost-effective and reliable means to store the large volumes of data that will be in most black box audit logs. However, storing highly sensitive information in the cloud may cause security and privacy concerns. Also, it remains an open regulatory question to what extent the cloud service provider and the organization that uses these services are responsible and legally liable for ensuring proper security measures are in place to safeguard this data (Kaufman 2009).

Finally, some have suggested that a blockchain, which is the distributed ledger that empowers bitcoin, could make a secure, decentralized and distributed corporate ledger. Once a transaction is published to the blockchain and confirmed as accurate, it cannot be reversed, altered or destroyed. Miners, for a small fee, continually ensure the security of the network and confirm the legitimacy of transactions passing through the blockchain. Moreover, blockchain transactions are pure peer-to-peer transactions.

Therefore, there is no intermediary involved nor third party trust concerns (Lazanis 2015).

4.6 Control Tags

Physical control tags (e.g., bar code readers and RFID tags) enable tracking and physical validation of audit objects. For example, control tags could log the passage of an inventory item through key control points in the business process (e.g., tracking an inventory item from the warehouse to the shipping company to its ultimate destination at a retail outlet). Control tags can be used to provide a continuous stream of audit information that can monitor the progression of physical objects through an organization's business process (Vasarhelyi 2004).

Similarly, data control tags use XML to append control information about the transaction. There are four unique types of data control tags:

1. Reliability Tags: tags that provide an ongoing reliability assessment of the control process that generated the transaction.
2. Tracer Tags: cookie crumbs tags that uniquely define a transaction, which are deposited in tracer receptacles at key processing points along the transaction's path.
3. Path Recording Tags: tags that are appended to the original transaction and record the key processing points that acted on it.
4. Information Control Tags: tags that contain other control information such as organizational placement, name of assurer, and related transactions.

A transaction can be simultaneously tagged with multiple types of the aforementioned control tags (Vasarhelyi 2005).

Nanosensors could be the next generation of control tags. They are extremely small devices, which can be used to detect optical, spatial, and chemical information. Nanosensors can also communicate using wireless networks and could be deployed in

clustered grids. For example, Nanosensors could be programmed to create smart packaging that detects microbes, toxins, and contaminants throughout the food processing chain, authenticate and track products, which prevents counterfeiting and diversion of products destined for a specific market, and monitor key environmental factors such as temperature and humidity (Bowles and Lu 2014).

4.7 Dashboard Reporting

Dashboard reporting is an extension of the **D**ecision **S**upport **S**ystems (DSS) and Executive Information Support research of the early 1990s. In 1989, Howard Dresner of the Gartner Group described dashboard reporting as a set of concepts and methods to improve business decision making using fact-based support systems (Power 2007). Essentially, dashboard reporting uses corporate databases to assess key performance indicators, compare key performance indicators to their metrics and perform trend analysis (e.g., sales for a line of business across years). Customized dashboards synthesizing deeper and more detailed operational, financial and marketing information could be a very valuable corporate asset. However, these dashboards require a defined structure, and rules to determine what data gets highlighted and escalation (Dewhurst and Willmott 2014).

These activities are very similar to the monitoring aspect of Continuous Auditing. The challenges of building a Dashboard report are similar to those encountered in building the Continuous Auditing system. For example both systems require complete, accurate and timely data at the right degree of granularity, which is most likely aggregated from multiple different systems (Warren 2003).

One example of a decision support system was implemented by the Royal Canadian Mounted Police (RCMP) to assess its Accounts Payable (AP) control framework. The system compared cost, quality and time-based performance measures for each AP office. For example, labor cost for accounts payable, the average number of errors per invoice and the average number of days to pay an invoice were calculated by extracting information for RCMP's ERP and Human Resource systems and compared across offices. Using these data analysis techniques the audit team uncovered control weaknesses and several instances of noncompliance with RCMP's policy (Coderre 2006).

4.8 Digital Agents

In the context of Continuous Auditing, (Woodroof and Searcy 2001) define a Digital Agent as software that acts on behalf of the auditor in a semi-autonomous manner to perform a service related to the subject matter being audited. Woodroof used an intelligent agent to continuously assure debt covenant compliance. This intelligent agent continuously extracts accounting information from the borrower's accounting system and compares it to the terms of its covenant agreement. Potential violations in the covenant agreement were flagged for auditors review.

CICA suggests that digital agents can be designed to remotely test transactions and controls on a continuous basis (CICA/AICPA 1999) However, (Debreceny and Gray 2001) state that financial information on the web may be difficult for digital agents to effectively use because of resource discovery (i.e., locating the financial statement on the web) and attribute identification (i.e., finding the appropriate financial statement line within the financial statement).

4.9 Extensible Business Reporting Language

E**X**tensible **B**usiness **R**eporting **L**anguage (XBRL) is an open data standard for electronic financial reporting that fosters greater transparency into financial statements. Using XBRL, organizations can capture financial information at any point in the business cycle (Coderre 2009). XBRL has the ability to tag each element on a financial statement or report with descriptive information, which facilitates the comparison of financial information between organizations. XBRL promises to improve accuracy of financial data, hasten its availability to capital markets, reduce the cost of providing financial data, facilitate paperless financial reporting, and provide more granular and comprehensive information (2009). Moreover, XBRL will reduce the need to rekey and reformat financial data when preparing financial documentation such as printed financial statements, HTML documents for the organization's website or an electronic EDGAR filing (Zarowin and Harding 2000).

One example of the analytic power of XBRL is FRAANK, an intelligent audit agent that converts an organization's quarterly and annual financial reports into a XBRL format and retrieves this organization's most recent stock price and earnings per share. FRAANK uses this financial information to calculate various accounting ratios and Z-score, which is a measure of bankruptcy risk. Consequently FRAANK reduces the complexity, cost and latency of converting financial information into a computer understandable format (Bovee, Kogan et al. 2005). Debreceny and Gray postulate that XBRL could be expanded to accommodate other types of financial reporting and speculates on an implementation time frame (Debreceny and Gray 2001). Vasarhelyi and Greenstein envision that XBRL will enable consolidation of distinct entities that

comprise a value chain, thereby facilitating end-to-end inter-organizational and value chain analysis (Vasarhelyi and Greenstein 2003). This would enable corporate stakeholders to understand the economics of the whole value chain and the effects of a particular event or trend on it.

Since the SEC mandated XBRL for regulatory filings, XBRL most likely will become the de facto standard in financial reporting. In 2009, organizations with a public float greater than $5 billion began using XBRL for their financial reporting. As of June 15, 2011, all publicly traded companies were required to use XBRL for their financial reporting (Aguilar 2008).

4.10 Workflow

A workflow is an orchestrated and repeatable pattern of business activity supported by systematic processes (Ko, Lee et al. 2009). There have not been a lot of research articles focusing on the workflow within the context of Continuous Auditing. However, workflow is used in commercial Continuous Auditing packages and intuitively seems to be a critical component for a Continuous Auditing system. For example, when a unique audit exception is identified either from an alarm or by some other means, a formal workflow process could be defined to ensure the audit exception gets resolved in a timely manner. At a minimum, a description of the audit exception the owner is responsible for resolving, a remediation plan, and a due date should be open for each audit exception. The remediation plan should be approved by the appropriate level of management, who will use this workflow module to monitor the audit exception's progress through the remediation process.

4.11 Third Party Solutions

Currently, there are several third-party Continuous Auditing software packages. ACL, Approva, CaseWare IDEA, MetricStream, Oversight Technologies and Trintech are a few examples of commercial Continuous Auditing systems. All of these products have predefined analytical methods for analyzing financial transactions, workflow management tools, sample business process control frameworks and ERP integration for extracting financial data. Approva, MetricStream and Trintech also include robust dashboard reporting and sample risk management control frameworks (Kuhn Jr and Sutton 2010).

CHAPTER 5

RESEARCH FRAMEWORK

5.1 Introduction

This chapter describes the research model that was developed based on factors identified in the literature review. This research model is both confirmatory and exploratory research. The research model is confirmatory because it builds on prior research to investigate whether the various proposed factors are useful in explaining relationships posited in the Continuous Monitoring domain space. However, this research model at its core is exploratory. It seeks to understand what are the most potentially fruitful Enterprise Risks and architectural components for a Continuous Monitoring implementation that would be used by management to monitor Enterprise Risks.

5.2 Confirmatory Research

Growing out of an extensive literature review related to Continuous Auditing the following two factors that may influence one's opinion on the usefulness of Continuous Monitoring were investigated:

> RQ1: What individual and organizational characteristics are related to the likelihood of favorable opinions toward the adoption of Continuous Monitoring?
>
> > H1: Employees of large auditing firms will be more resistant to Continuous Monitoring than the general population. Research has indicated that a group's resistance to a new system will increase if they perceive that it could reduce their power (Markus 1983). Continuous Monitoring systems could jeopardize the big four accounting companies' traditional business model.
> >
> > H2: Continuous Monitoring is more likely viewed favorably in companies with larger total revenue. Research has indicated that a high-level of investment is a key prerequisite to successful Continuous Monitoring implementations (Fedorowicz 2008).

5.3 Exploratory Research

Ultimately, this research model seeks to understand what is the most potentially fruitful domain space and technical architecture for an Enterprise Continuous Monitoring implementation. By using qualitative methods, this research strives to gain expert consensus on the ideal Enterprise Risks and technical architecture. This complex and contextual decision-making process lends itself to qualitative research, which seeks to drive to consensus among an expert panel. Specific research questions include:

- RQ2: Which Enterprise Risks are most amenable to Continuous Monitoring?
- RQ3: Which Continuous Monitoring architectural components are perceived as most applicable to which types of Enterprise risks?
- RQ4: How does participation in an online Delphi process change the initial viewpoints of the participants?

5.4 Methodology

The research methodology was a snowballing Collaborating Design Delphi research study targeting professionals with experience in risk management, accounting, and/or Information Systems. The traditional Delphi method is a structured, anonymous and multi-round survey process, where expert opinion is aggregated and disseminated to participants in subsequent rounds (Linstone 1975). In Round one, a questionnaire was anonymously posed. In subsequent rounds, the results from the previous round were aggregated and presented to the expert panel, which had the opportunity to revise their original answers in light of this new information. Snowballing allowed the expert panel to suggest other experts to participate in the research study. The researcher reviewed the qualifications of the suggested additions to the expert panel. When they were consistent

with the desired profile of the research study, the researcher asked permission to use the name of the recommender in the invitation to the research study.

The Delphi research method is well suited for this research problem. The Delphi research method is designed to drive convergence between conflicting views. Moreover, the Delphi research method has a long history of being used for long-range technology predictions (Gordon and Helmer 1964). Expert opinions have proven to be the best and, in some cases, the only source of available information, for forecasts in highly volatile and uncertain domain spaces like this one (Linstone 1975; Linstone and Turoff 2011) . Finally in general, this method overcomes the halo and bandwagon decision traps (Rowe, Wright et al. 1991) and produces more accurate forecasts than individuals on the average (Parenté, Anderson et al. 1984).

Since Continuous Monitoring is a relatively new and niche concept, snowballing facilitated soliciting an adequate number of participants with sufficient qualifications to participate in this research. Moreover, Collaborative Design has proven useful not only to the Continuous Monitoring domain space, but also other emerging areas of Information Systems research, where academic researchers have the objective of shaping practices as opposed to just describing them (Alles, Kogan et al. 2013).

5.5 Participants

In order to select suitable experts for the Delphi panel, the researcher's personal and professional networks were scrutinized looking for individuals who have expertise in either risk management, accounting and/or Information Systems. The ideal panel member had at least five years of professional experience and some knowledge of risk management, Information Systems or auditing. Over 200 such individuals were

identified from the researcher's professional network. These individuals were sent an email with a link to participate in this research. The researcher also promoted this study on Linkedin and hired Suvata, which is a target research firm, to attract additional participants. The researcher's dissertation committee had extensive personal and professional networks that were solicited as well. Moreover, each participant had the opportunity to invite additional experts to participate during Round 1. The minimally sufficient sample size for this Delphi was 50 total participants, of which at least 15 were required to be corporate risk managers.

5.6 Procedures

Questionnaires and procedures were submitted to the NJIT IRB prior to their use. Before distributing questionnaires, pretests were carried out on a small number of subjects. All selected participants received an email invitation from the researcher with a hyperlink to the Round 1 questionnaire. This questionnaire had three sections: 1) A consent form, 2) Demographic Questions, and 3) Scenario Generation Questions, which allowed the participants to evaluate the importance of each risk and the feasibility of continuously monitoring it. All participants that completed this questionnaire were invited via an email to participate in subsequent rounds.

Round 2 presented three risk scenarios and let participants evaluate the desirability and feasibility of the proposed measures and opine on how useful Continuous Monitoring would be to monitoring these risk scenarios. Round 3 presented the key assumptions collected in Round 2 and allowed participants to change their Round 2 answers in light of these assumptions. Each round lasted approximately one to two

months. This research study took approximately 6 months. The below figure summarizes the process.

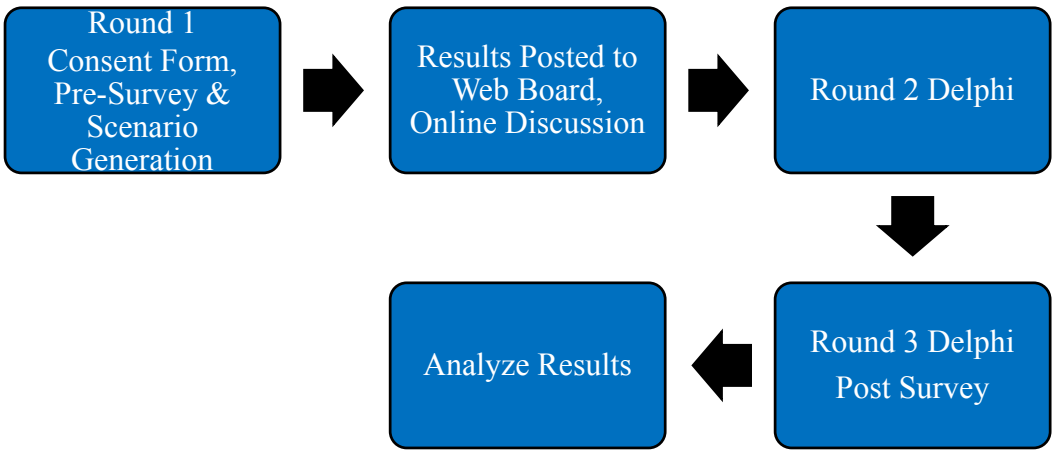

Figure 5.1 Summary of research method.

Great care was taken to ensure that this research study would not have any adverse effects on its participants. Prior to conducting this research study, the researcher, who is a NJIT Ph.D. student, completed the online training course in the protection of human subjects offered by the US Department of Health and Human Services. Initial questions and consent forms were reviewed and edited by his Ph.D. committee. Moreover, participation in the survey is completely optional and is targeted to working professionals over the age of 21. Finally, participants could choose to terminate their involvement in this research study at any time for any reason.

Reasonable safeguards were in place to protect the anonymity of the participants. Numerical IDs were assigned to participants' survey results. The numerical ID mapping to the participant's name remain strictly confidential. This key as well as all the raw research data, including the survey responses are stored on the researcher's password-

protected and encrypted computer. Participants were informed that the responses might be summarized and, possibly, disseminated to the professional community. However, the researcher took special care to prevent responses from being traced back to individual participants. Only participants that granted explicit permission could have their name listed in subsequent publications.

Before being distributed to participants all questions were approved by the Institutional Review Board (IRB). All of the IRB suggested modifications were incorporated. Then, the survey questions were drafted and piloted with several test participants. The pilot was designed to ensure that questions were understandable and clear.

5.7 Measurement and Analysis

For Research Question 1, attitudes towards Continuous Monitoring were grouped into three buckets 1) those who have worked for a Big 4 auditing firm. 2) those that are currently working for the largest companies in terms of revenue and do not work at a Big 4 auditing firm 3) those that are currently working for the smallest companies. An ANOVA was used to determine if there is a statistical difference for the perceived usefulness of a Continuous Monitoring system among these groups.

For Research Question 2, the ideal Enterprise Risk for Continuous Monitoring techniques would have a continuous stream of analyzable electronic data, have a domain space that does not overly rely on human judgment nor contain competing objectives, have a predictive model that is cheap to construct and improves the accuracy, reliability, and/or timeliness of risk predictions over what is currently available via expert decision-making, and be a useful measure to a risk practitioner. The mean and standard deviation

were calculated for Round 2's questions. The second part of each question was qualitatively analyzed to identify the key assumption themes that were presented in subsequent rounds of the Delphi. In Round 3, the quantitative and qualitative summary of each question was provided for each of the Likert scale questions. Specifically the mean and standard deviation of the first part of each question as well as a summary of the key assumption themes from the second part were presented. In light of this new information, the participants were asked to evaluate the assumptions that underlay different answers (using a Likert scale and open-ended comments) and then to reevaluate their answers to the first part of each question (i.e., the Likert scale question) for the same risk scenarios. The Enterprise Risks were ranked by how much they lend themselves to Continuous Monitoring techniques. These questions were structured such that risks with higher aggregate average Likert scores were more amenable to Continuous Monitoring techniques than those with lower average Likert scores. To calculate the overall auspiciousness for using Continuous Monitoring for a specific risk scenario, all of its Likert- scale questions were averaged together. The Enterprise Risk that on average had the highest Likert score was deemed the best Enterprise Risk for Continuous Monitoring.

For Research Question 3, participants were asked to identify the architectural components that would form the basis of a Continuous Monitoring System for a particular Enterprise Risk. A Kruskal-Wallis test was used to determine whether there were differences among the usage of architectural components across different Enterprise Risks. For each Enterprise Risk, participants were asked to suggest other architectural components that were not listed. These suggestions were qualitatively analyzed to assess the completeness of the architecture literature review in Chapter 4.

After the final round, the questions' means and standard deviations were compared between Rounds 2 and 3. If the Delphi were driving towards consensus, the standard deviations would be reduced in Round 3. For Research Question 4, the answers to the pre-test and post-test Continuous Monitoring perceived business value question were compared with a t-test to see if the study materially influenced the participant's opinions on Continuous Monitoring. Finally, data analysis was performed to determine whether there were any latent relationships between the demographic information and the perceived business value of Continuous Monitoring.

CHAPTER 6

RESEARCH RESULTS

6.1 Round 1

In Round 1, 217 potential participants that were selected from the researcher's professional network received an email invitation to participate in this research study. The Round 1 survey was hosted by Surveymonkey.com and was open from June 30th 2014 to August 11th 2014. The complete survey is listed in Appendix A.

To promote this research study all potential participants were allowed to recommend additional participants regardless of whether or not they actually participated in the research study. Public invitations were also posted on a couple of LinkedIn groups: Continuous Controls Monitoring and Continuous Audit. Finally Survata, which is a targeted survey firm, was retained to identify and solicit additional participants.

At the end of Round 1, there were 184 fully completed responses. There were an additional 65 surveys that were started, but not completed, and two surveys where the respondents answered, "I don't know" to every question. These surveys were disregarded from all subsequent data analysis. For the completed surveys, respondents had an average of 13 years of I.T. experience, and six years of risk management and internal/external audit experience. 29 (16% of total) were C-Level executives (e.g., CEOs, CTOs CIOs, etc.), 30 (16% of the total) were senior managers, 72 (39% of the total) were middle management, and the other 53 (28 % of the total) were either in another role or not employed. The Table 6.1 has the complete distribution.

Table 6.1 Respondent's Position Distribution

Position	Count	%
C-Level Executive	29	16%
Senior Management	30	16%
Supervisor / Middle Management	72	39%
Other	34	18%
Not Employed	19	10%
Total	**184**	**100%**

There were 119 respondents (65% of the total) that identified themselves as male, 63 (34% of the total) respondents that identified themselves as female and 2 respondents that preferred not to identify their gender. There were 95 respondents, 52% of the total that completed their bachelor's degree, 56 respondents (30% of the total) that completed their master's degree, and 3 respondents (2% of the total) completed their doctorate. The Table 6.2 has the complete distribution.

Table 6.2 Respondent's Education Distribution

Highest Education	Count	%
High School	28	15%
Bachelors	95	52%
Masters	56	30%
Doctorate	3	2%
None of the above	2	1%
Total	**184**	**100%**

Age was pretty evenly distributed between the ages of 21 and 64. 38 (21% of total) respondents stated they were between 21 and 34 years old, 43 (23% of total) were between the ages of 35 and 44 years old, 54 (29% of total) were between 45 and 54 years old, and 42 (23% of total) were between 55 and 64 years old. There were only 7 (4% of total) respondents between the ages of 65 and 74 years old, and no respondents selected

"75 years or older" or the "Prefer not to answer" categories. The Table 6.3 has the complete distribution.

Table 6.3 Respondent's Age Distribution

Age Group	Count	%
21-34 years old	38	21%
35-44 years old	43	23%
45-54 years old	54	29%
55-64 years old	42	23%
65-74 years old	7	4%
Total	**184**	**100%**

The respondents worked in many different industries. 32% of the respondents selected "Other" for their industry. Moreover, the ten industries listed on the survey each had three or more respondents. Manufacturing and Banking/Finance had the most entries with 23 each, which was 12% of the total. Transportation had the fewest respondents with three. Table 6.4 has the complete distribution. Ten respondents worked at a Big 4 accounting firm, while 174 have not. Overall, the response rate from Big 4 accounting companies was surprisingly low relative to other industries. Some respondents that worked for a Big 4 accounting firm commented that their firm had a stated policy prohibiting participation in unsanctioned accounting research studies.

Table 6.4 Respondent's Position Distribution

Industry	Count	%
Other	59	32%
Manufacturing	23	12%
Banking/Finance	23	12%
Not Currently Employed	16	9%
Government	11	6%
Education	10	5%
Communications	10	5%
Healthcare	10	5%
Insurance	9	5%
Retail	6	3%
Hospitality	5	3%
Transportation	3	2%
Total	**184**	**100%**

The respondents tended to work in larger companies. "Over a billion", which was both the largest revenue category and also the most frequently selected category on the survey, had 47 respondents (26% of the total). The other five revenue levels all had at least ten respondents each. 27 respondents (15% of the total) did not know their company's revenue size. The Table 6.5 has the complete distribution.

Table 6.5 Respondent's Company Size Distribution

Company Size	Count	%
Under $1M	22	12%
Between $1 and $10 Million	23	13%
Between $10 and $100 Million	36	20%
Between $100 and $500 Million	19	10%
Between $500 Million and $1 Billion	10	5%
Over $1 Billion	47	26%
Not sure / Don't know	27	15%
Total	**184**	**100%**

6.1.1 Attitudes Towards Continuous Monitoring

Overall, the respondents had a very positive view of Continuous Monitoring. There were 73 respondents (39% of the total) that believed Continuous Monitoring is "Very Likely" to provide material business value and 83 respondents (44% of the total) believe Continuous Monitoring is "Likely" to have material business value. Conversely only two respondents (1% of the total) believed that Continuous Monitoring was unlikely to provide material business value. Table 6.6 has the complete distribution.

Table 6.6 Respondent's Belief that Continuous Monitoring Could Add Value

Company Size	Count	%
Very likely	73	40%
Likely	83	45%
Neutral	26	14%
Unlikely	0	0%
Very unlikely	2	1%
Total	**184**	**100%**

Questions 14 and 15 determine an Enterprise Risk's feasibility and desirability respectively. The "Don't know" answers were filtered out for both questions and their feasibility and desirability scores were averaged together. In aggregate, the top three Enterprise Risks that the participants believed lend themselves to a Continuous Monitoring system are (1) Computer Crime (2) Credit, Market and Liquidity Risk (3) Damage to Brand and Reputation. The bottom three risks were Legal, Regulatory and Commodity Price Risk. Table 6.7 has the complete rankings.

Table 6.7 Average Ranking by Enterprise Risks

Average Ranking by Enterprise Risks (Lower is better)	Desirable*	Feasible**	Average Desirability & Feasibility
Computer Crime	1.83	2.14	1.98
Credit, Market and Liquidity Risk	2.02	2.15	2.08
Damage to brand/reputation	2.05	2.21	2.13
External Business interruption	2.07	2.24	2.15
Surprise Competitive Threats	2.02	2.29	2.16
Economic Volatility	2.10	2.33	2.21
Internal Business interruption	2.09	2.35	2.22
Legal Risks	2.13	2.36	2.24
Regulatory	2.13	2.38	2.26
Commodity Price Risk	2.21	2.37	2.29
*Scale: 1-Very Desirable; 2-Desirable; 3-Possibly Desirable; 4-Undesirable; 5-Very Undesirable		**Scale: 1-Very Feasible; 2-Feasible; 3-Possibly Feasible; 4-Unfeasible; 5-Very Unfeasible	

6.1.2 RQ1: Adoption Characteristics

Research Question 1 attempts to determine the individual and organizational characteristics related to favorable opinions about Continuous Monitoring. Based on the literature review, the size and type of a company were hypothesized to influence the perception of Continuous Monitoring. Other things being equal, working at a Big 4 audit firm was hypothesized to lead to a more unfavorable perception of Continuous Monitoring while working at another large company was hypothesized to lead to a more favorable perception. Prior research has indicated that Continuous Monitoring systems could jeopardize the Big four accounting companies' traditional business model, which would make them selfishly more cynical of this technology, and that a high-level of investment required for Continuous Monitoring implementations, would make this technology more appealing to large companies that can afford it compared to small companies that could not.

Question 13 is the dependent variable. It asked, "To what extent do you believe that Continuous Monitoring has the potential to provide material business value to today's companies?" The complete distribution of answer choices was shown above in Table 6.6. The Likert score scale was

0 – Don't Know (not used in the analysis).
1 – Very Unlikely
2 – Unlikely
3 – Neutral
4 – Likely
5 - Very Likely

"Don't know" responses were dropped from the mean and standard deviation calculations, because this analysis focused only on participants that were confident in their answers, which is standard protocol for this type of analysis. The Ryan-Joiner normality test confirms that this variable is normally distributed at an $\alpha = 0.05$ ($p=0.10$). However, this question is substantially skewed toward the positive end. Dropping "0-Don't Know" responses from the sample, the sample's mean is 4.22 and its standard deviation is 0.77.

The independent variables are Question 10 and Question 11. Question 10 asked, "Are you employed by PWC, Deloitte & Touche, Ernst & Young and/or KPMG?" (i.e., the Big 4 Accounting firms). The answer choices were "Yes" and "No". Question 11 asked, "How large is your current employer in terms of Total Annual Revenue?" The answer choices were

Under $1 Million

> $1 Million and <= $10 Million

> $10 Million and <= $100 Million

> $100 Million <= $500 Million

> $500 Million <= $1 Billion

Over $1 Billion

Not sure / Don't know

The "I Don't know" responses for Questions 11 and 13 were dropped. Table 6.8 shows the Likert score distribution across these categories.

Table 6.8 RQ1 Distribution by Likert Scale

	Very Unlikely 1	**Unlikely 2**	**Neutral 3**	**Likely 4**	**Very Likely 5**	**N**
Big 4	10%	10%	30%	50%	10%	10
Not Big 4	1%	14%	45%	40%	1%	157
$1B or more	2%	9%	38%	51%	2%	45
Under $1B	0%	17%	49%	34%	0%	102

The means are in the hypothesized order: Big 4 the lowest (i.e., 4.10) and "1B or more" the highest (4.36). See the below figure.

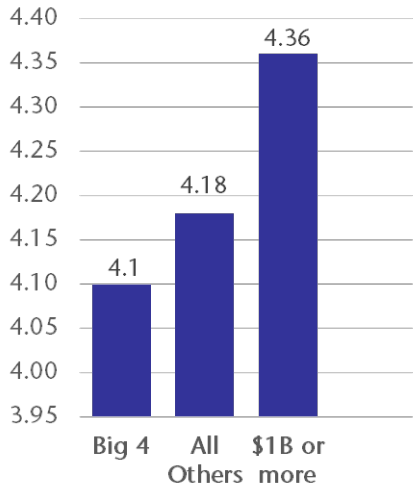

Figure 6.1 Mean by Business Case.

The Point Biserial Correlation Coefficient for revenue size is 0.11, which means there is a slight positive correlation between revenue size and increased Likert score for perceived usefulness of Continuous Monitoring. The Point Biserial Correlation Coefficient for a Big 4 audit firm is -0.04, which means there is a very small negative correlation between working at a big audit firm and the perceived usefulness of Continuous Monitoring. Table 6.9 has the summary statistics for these groups.

Table 6.9 RQ1 Summary Statistics

	N	Mean	Stdev
Big 4	10	4.10	1.29
Not Big 4	147	4.23	0.74
$1B or more	45	4.36	0.83
Under $1B	102	4.18	0.70
All	**157**	**4.22**	**0.78**

Even though the means are in the hypothesized order, this result was not statistically significant. A one-way analysis of variance (ANOVA), which is a statistical method that analyzes variations in means among disparate groups, was calculated for the three groups: 1) "Companies $1 Billion or more in Revenue", 2) "Companies less than a 3) $1 Billion in revenue", and "Big 4 Accounting firms", which by their nature are over $1 Billion in revenue. The analysis was not significant at an $\alpha = 0.05$ ($p = .39$), when using the single question indicator of attitude toward Continuous Monitoring.

6.1.3 Constructing a Desirability Index

In order to construct an alternative measure of business value, a Factor analysis, which is a statistical method that examines correlations among observed variables to extract a few latent variables, was run to create a Desirability index. Question 15 solicited opinions on how desirable Continuous Monitoring would be for the Enterprise Risks identified in the

literature review. The following sample set manipulations where made to clean the data and consolidate categories that had sparse data points:

- Respondents that answered, "I don't know" to any Desirability or Feasibility question were dropped from the sample.
- Respondents that answered "None of the above" to Question 8 were dropped because of their small sample sizes. Those that answered "Doctorate" where grouped into "Masters+."
- Respondents that answered, "Prefer not to answer" to Question 7, which dealt with Gender, were dropped, because of its small sample size.
- Question 9, which was the Industry question, responses that were either "Retail", "Hospitality", or "Transportation" were recoded as "Other".
- Question 5 responses, which captured the amount of Risk Management, Information Systems, and Audit Experience the respondents had, were collapsed into the following categories "None", "<= 5", ">5 and <= 10" ">10 and <=20", "20+" years.

In total, 17 respondents were removed from the sample and 12 answers to Question 9 were recoded as "Other". Table 6.10 summarizes the resulting distribution.

Table 6.10 Desirability Distribution by Likert Scale

Enterprise Risk	1	2	3	4	5
15.a: Economic Volatility	30%	38%	27%	5%	0%
15.b: Regulatory	31%	35%	27%	5%	1%
15.c: Competitive Threats	37%	37%	20%	5%	1%
15.d: Market	36%	35%	25%	4%	1%
15.e: Reputation	34%	37%	22%	7%	1%
15.f: Legal	37%	26%	28%	8%	1%
15.g: External Interruption	37%	33%	23%	4%	2%
15.h: Internal interruption	32%	38%	22%	5%	2%
15.i: Commodity	28%	37%	27%	7%	1%
15.j: Computer Crime	48%	32%	16%	3%	2%
1-Very Desirable; 2-Desirable; 3-Possibly Desirable; 4-Undesirable; 5-Very Undesirable					

The Factor analysis was run on this same sample set of 167 respondents. The one variable Factor analysis explained 67% of the variance and measures the Desirability of using Continuous Monitoring across this set of Enterprise Risks. Table 6.11 has the

loading factors, which demonstrate a strong correlation with Question 15's desirability variables and measures the desirability of using Continuous Monitoring across this set of Enterprise Risks.

Table 6.11 Loading Factors from Factor Analysis

Variable	Loading Factors
Economic Volatility	0.72
Regulatory	0.79
Competitive Threats	0.84
Market	0.77
Reputation	0.78
Legal	0.85
External Interruption	0.85
Internal Interruption	0.82
Commodity	0.85
Computer Crime	0.83

This desirability index has a Cronbach's alpha of 0.95, which means that it is strongly internally consistent. Its mean is 2.47 and standard deviation is 0.95.

A one way ANOVA was individually run between the demographic variables and Desirability Index. No variables were significant at $\alpha = 0.05$. However, Years of Audit Experience was significant at $\alpha = 0.10$. Generally speaking, the more years of audit experience the participant had the more desirable they thought Continuous Monitoring would be. Big 4, Years of Information Management Experience, Years of Risk Management Experience, Education, Revenue, Role, Industry, Gender and Age variables were not significant at an $\alpha = 0.10$.

Table 6.12 Desirability Index ANOVA P-Value and R Square Values

Variable	P-Value	R-Square
Years of Auditing Experience**	0.06	5.34
Education	0.19	2.04
Years of Risk Management Experience	0.22	3.49
Role	0.38	2.56
Age	0.42	2.36
Revenue	0.44	3.55
Industry	0.45	4.75
Years of Information Management Experience	0.51	2.00
Gender	0.87	0.02
Big 4	0.95	0.00
**Signification at $\alpha = 0.10$		

6.1.4 Constructing a Feasibility Index

In order to construct an alternative measure of business value, a Factor analysis was run on the feasibility variables from Questions 16. Question 16 solicited opinions on how feasible Continuous Monitoring would be for the Enterprise Risk identified in the literature review. Table 6.13 summarizes this distribution.

Table6.13 Feasibility Distribution by Likert Scale

Enterprise Risk	1	2	3	4	5
16.a: Economic Volatility	25%	37%	31%	8%	0%
16.b: Regulatory	23%	38%	29%	10%	0%
16.c: Competitive Threats	25%	34%	34%	7%	1%
15.i: Commodity Price	25%	31%	33%	10%	1%
15.j: Computer Crime	32%	30%	34%	4%	0%
15.g: External interruption	27%	23%	41%	8%	1%
15.h: Internal Business	24%	29%	37%	9%	1%
15.f: Legal	24%	28%	35%	11%	1%
15.d: Market	26%	25%	44%	5%	1%
15.e: Reputation	28%	32%	35%	5%	0%
1-Very Feasible; 2-Feasible; 3-Possibly Feasible; 4-Unfeasible; 5-Very Unfeasible					

The Factor analysis was run on the same sample set of 167 respondents described in Subsection 6.1.3. The one variable Factor analysis explained 41% of the variance. Table 6.14 has its loading factors, which demonstrates a strong correlation with Question

16's feasibility variables and measures the feasibility of using Continuous Monitoring across this set of Enterprise Risks.

Table 6.14 Loading Factors from Factor Analysis

Variable	Loading Factor
Economic Volatility	0.63
Regulatory	0.66
Competitive Threats	0.70
Market	0.55
Reputation	0.59
Legal	0.60
External Interruption	0.66
Internal Interruption	0.72
Commodity Risk	0.64
Computer Crime	0.61

This feasibility index has a Cronbach's alpha of 0.84, which implies that it has good internal consistency. Its mean is 3.55 and standard deviation is 0.95

A one way ANOVA was run between the demographic variables and Feasibility Index. Years of Audit was significant at $\alpha = 0.05$ and Years of Risk Management Experience was significant at $\alpha = 0.10$. Generally speaking, the more years of audit and/or risk management experience, the more feasible the participant thought Continuous Monitoring would be. Big 4, Years of Information Management Experience, Education, Revenue, Role, Industry, Gender and Age variables were not significant at an $\alpha = 0.10$. Big 4, Years of Information Management Experience, Education, Revenue, Role, Industry, Gender and Age variables were not significant at an $\alpha = 0.10$.

Table 6.15 Feasibility Index ANOVA P-Value and R Square Values

Variable	P-Value	R-Square
Years of Auditing Experience*	0.00	11.61
Years of Risk Management Experience**	0.08	5.04
Education	0.38	1.16
Revenue	0.42	3.64
Big 4	0.46	0.33
Years of Information Management Experience	0.48	2.13
Gender	0.85	0.02
Role	0.90	0.64
Age	0.91	6.10
Industry	0.93	1.88
* Significant at $\alpha = 0.05$ ** Significant at $\alpha = 0.10$		

6.1.5 Exploratory Data Analysis

Round 1's data was also examined to determine whether there are any latent relationships that were not explicitly indicated by the literature review. A one way ANOVA was run on the same sample set of 167 respondents described in Subsection 6.1.3. The ANOVA individually compared demographic variables and Question 13 that measures business value. Question 13 is "To what extent do you believe that Continuous Monitoring has the potential to provide material business value to today's companies?" Years of Auditing Experience and Years of Risk Management Experience were significant at $\alpha = 0.05$. Big 4, Years of Information Management Experience, Education, Revenue, Role, Industry, Gender and Age variables were not significant at an $\alpha = 0.10$.

Table 6.16 Perceived Business Value ANOVA P-Value and R Square Values

Variable	P-Value	R-Square
Years of Auditing Experience*	0.01	8.27
Years of Risk Management Experience*	0.02	6.72
Big 4	0.15	1.24
Years of Information Management Experience	0.17	3.88
Education	0.69	0.45
Revenue	0.75	2.12
Role	0.88	0.72
Industry	0.89	2.22
Gender	0.96	0.00
Age	0.98	0.24
* Significant at $\alpha = 0.05$		

For both Risk Management and Auditing, having more than five years of experience seems to affect the perceived business value for Continuous Monitoring. Participants that had less than five years' experience in these respective areas tended to have worse perception of Continuous Monitoring value proposition than their more experienced counterparts did. For Risk Management five to ten years of experience had the highest perceived value of Continuous Monitoring. The perception decreases in the ten to 20 year range, and fell again in the 20+ year range. Similarly, for Auditing, the five to ten years of experience had the highest perceived value of Continuous Monitoring and the perception dipped slightly with ten to 20 years of experience. However, for auditing, 20+ years of experience had the highest perceived business value (see below table).

Table 6.17 Mean Perceived Business Value by Years of Experience

	Risk Management		Auditing	
Years of Experience	**Average Business Value Likert**	**Count**	**Average Business Value Likert**	**Count**
None	2.0	57	1.9	57
<=5	1.8	42	1.9	53
>5 & <=10	1.5	36	1.5	33
>10 & <=20	1.6	26	1.6	15
20+	1.8	6	1.3	9
Total	**1.8**	**167**	**1.8**	**167**
Scale: 1-Very Likely, 2-Likely, 3-Neutral, 4-Unlikely, 5-Very Unlikely				

Performing a t-test on these variables when they are bisected into two groups: "less than or equal to five years of experience" and "greater than five years of experience", yields significant results at $\alpha = 0.05$ For Risk Management and Auditing experience, the t-test yields a p-value = .00. This implies that having more experience in either Risk Management and/or Auditing significantly affects the perceived business value of Continuous Monitoring. It appears that the more experience in these areas, the higher the perceived value of Continuous Monitoring.

6.1.6 Differences between Solicitation Methods

There were two methods used to solicit participants: 1) the researcher's professional network and 2) Survata, which is a targeted research firm. For Round 1 there were 150 participants in the Survata pool and 17 participants in the researcher's pool. They were compared along several dimensions to determine whether there were statistical differences between the solicitation methods. Specifically, these pools were compared using a one-way ANOVA along the following dimensions: perceived value of Continuous Monitoring (Question 13), company revenue size (Question 11), role (Question 12) and education (Question 8). See Appendix A for exact questions.

Between the pools, education was the only dimension with a statistical difference at an α = 0.05 (see below table).

Table 6.18 Mean Business Value by years of Risk Management and Audit Experience

Question #: Variable	Researcher Mean	Survata Mean	P
Q8: Education*	2.14	2.59	0.01
Q11: Company Revenue	3.26	3.12	0.80
Q12: Role	1.19	1.18	0.95
Q13: Perceived Business Value Proposition	1.59	1.77	0.33
* Significant at α = 0.05			

Table 6.19 contains the Likert score to answer choice mapping by question.

Table 6.19 Likert score to Answer Choice Mapping

Likert Value	Question 8 Education	Question 11 Revenue	Question 12 Role	Question 13 Value Prop
0	None of the above	Not sure	Not Employed / Other	Very likely
1	High School	Under $1M	Middle Manger	Likely
2	Bachelors	$1 - $10 Mil	Senior Manager	Neutral
3	Masters+	$10 - $100 Mil	Executive	Unlikely
4		$100 - $500 Mil		Very unlikely
5		$500 Mil - $1 Bil		
6		Over $1 Bil		

6.1.7 Building Round 2's Scenarios

Question 16 was qualitatively analyzed for potential scenarios for Round 2. The following Enterprise Risk Taxonomy was used

- Economic Volatility or Slowdown: Another major financial crisis (e.g., Mortgage default) and/or downturn. Recent examples include weakness in the Eurozone, projected slowed economic growth forecast in India and China, persistent fiscal changes in Japan, and elevated worldwide unemployment rate, reoccurring financial crisis, failure of major countries to pay their debt.
- Regulatory pressure and/or changes in regulatory environment: Basel III, SOX, Dodd-Frank, Solvency II, foreign corrupt practices legislation, local privacy, investigation by government agency or regulatory body & laws and the International Financial Reporting Standards, Health Care reforms.

- Surprise Competitive Threats: New and, perhaps better, competitors and/or products in the marketplace change in consumer trends and technological advancements (i.e., product obsolesces), increased global competitive pressures, aggressive competitive tactics (such as price wars), mergers and acquisitions.
- Credit, Market and Liquidity Risk: The risk that borrows will default on their commitments. The risk that an investor will experience losses as result of participating in financial markets. The risk of loss resulting from being unable to trade a security or asset quickly.
- Damage to brand/reputation: product recalls, regulatory challenges (e.g., JP Morgan Chase), involvement in a corporate or personal scandal (e.g., Martha Stewart), failure of core strategy or product (e.g., Blackberry), unable to meet demand for successful product, being flamed on social media.
- Legal Risks: Customer and employee lawsuits.
- External Business interruption: Infrastructure failures (e.g., electricity and telecommunication network failures), financial market failures (closing of key markets), loss of computer infrastructure, transportation strikes, criminal attacks, or embargos.
- Internal Business interruption: For example strike or slowdown, accidents, fraud, workplace violence, industrial accidents (e.g., nuclear power plant explosion of materials or fires).
- Commodity Price Risk: Crude oil, Natural gas, shortages that lead to price run-ups.
- Computer Crime: Financial losses from virus and malicious code, proprietary or customer information can be stolen via hacking or internal theft (e.g., target customer credit cards); malicious software can disrupt operations of essential services such as security, defense, power plants, as well as banking, commerce, etc.

The qualitative analysis revealed that 58 respondents did not provide business scenarios. The computer crime category had the largest number of suggested scenarios. 32 respondents suggested a specific Computer Crime scenario (e.g., hacking, IP theft, etc.) as the most auspicious area for a Continuous Monitoring system. Most suggested scenarios dealing with protecting customer and credit card data from hackers. Both the 2014 Target and 2012 Sony intrusions were suggested as possible scenarios. Other more novel suggestions included preventing a terrorist group from infiltrating a highly valuable

security defense area such as a nuclear power plant, detecting phishing schemes on social media sites and monitoring employee access patterns to prevent data theft.

Several suggested more traditional Continuous Monitoring Scenarios in the areas of Operations, Fraud Detection and Compliance, which is where Continuous Monitoring has been routinely used for some time now. Some example scenarios include monitoring for operational processes for failure, fraud, audit exceptions, business interruptions and long tailed risk. However, there were also some novel suggestions. Two respondents suggested using Continuous Monitoring to monitor social media to detect potential reputational risks and/or looming public relations crises. Another two respondents suggested using Continuous Monitoring to monitor the speed of operational and production processes. Finally, another two respondents suggested using Continuous Monitoring in the health care field. One suggested monitoring medical records for potential early warning signs of a serious medical condition. The other suggested using Continuous Monitoring to ensure a hospital's compliance with governmental mandates around health care. These novel scenarios could be the basis of future research in Continuous Monitoring. Table 6.20 has the complete distribution.

Table 6.20 Qualitative Categorization of Scenario Generation Question

Category	N	%
No Scenario Provided	58	31.52%
Computer Crime*	32	17.39%
Operations**	24	13.04%
Other	20	10.87%
Economic Volatility*	15	8.15%
Internal Fraud/Thief**	11	5.98%
External Business interruption*	8	4.35%
Surprise Competitive Threats*	7	3.80%
Regulatory*	3	1.63%
Credit, Market and Liquidity Risk*	2	1.09%
Legal Risks*	1	0.54%
Damage to brand/reputation*	1	0.54%
Compliance**	1	0.54%
Internal Business interruption*	1	0.54%
Commodity Price Risk*	0	0%
Total	**184**	**100.00%**
Enterprise Risks*		
Traditional Continuous Monitoring Risk**		

Computer Crime, Economic Volatility, and Surprise Competitive Threat were chosen to be studied in Round 2. The Harvard Business Case repository was searched for representative business cases that fit these Enterprise Risks. After a thorough review, the following cases were selected: Sony's 2012 Cyber Intrusion for Computer Crime, Bear Stearns' Implosion for Market Risk, and RIM's loss of Competitive Advantage for Damage to brand and/or reputation. These cases were summarized and presented in Round 2. These Business Cases are listed in Appendix B.

6.2 Round 2

The 188 respondents that completed Round 1 were sent an email invitation to the Round 2 survey. The Round 2 survey was hosted by Surveymonkey.com and was open from September 29, 2014 to November 10, 2014. Round 2 had 81 respondents that completed the entire survey. The dropout rate between Round 1 and Round 2 was 57%. Round 2 presented examples of the top three Enterprise Risks identified in Round 1. The Sony scenario dealt with computer crime. The Bear Stearns scenario dealt with operational risk. The RIM scenario dealt with strategic risk. The complete survey is listed in Appendix B.

6.2.1 RQ2: Auspicious Enterprise Risks

Research Question 2 seeks to determine which Enterprise Risks are most amenable to Continuous Monitoring. Likert-type questions were constructed to measure the detailed factors that could lead to a successful Continuous Monitoring system. Six factors were identified based upon the literature review:

1. Cost of human judgment,
2. Cost of building a predictive model,
3. Availability of digital data,
4. Proficiency of human judgment to detect risk,
5. The probability a predictive model can be built and,
6. The performance of the best predictive model compared to expert human judgment.

The Likert scale was constructed such that a higher Likert score on a question indicated a more advantageous scenario for Continuous Monitoring. The same Likert questions were asked for all three business scenarios. Table 6.21 has the Likert Scale for each question.

Table 6.21 Likert Scale by Question

	0	1	2	3	4	5
Cost Human Judgment	No Judgment / I don't know	Extremely cheap	Relatively cheap	Reasonable	Moderately expensive	Prohibitive expensive
Cost Predictive Model	No Judgment / I don't know	Prohibitive Expensive	Moderately expensive	Reasonable	Relatively cheap	Extremely cheap
Digital Data	No Judgment / I don't know	None or very little of the data needed is in a digital form	Some of the relevant data is available digitally	About half of the relevant data is available digitally	Most of the relevant data is available digitally	All the relevant data is available digitally
Human Judgment Detect Risk	No Judgment / I don't know	Definitely Infeasible	Possibly Infeasible	Feasible	Possibly Feasible	Definitely Feasible
Predictive Model Can be Built	No Judgment / I don't know	Definitely Feasible	Possibly Feasible	Feasible	Possibly Infeasible	Definitely Infeasible
Predictive Model compared to Human	No Judgment / I don't know	Far inferior in terms of accuracy, consistency and/or timeliness of predictions	Moderately inferior in terms of accuracy, consistency and/or timeliness of predictions	About the same	Moderately superior in terms of accuracy, consistency and/or timeliness of predictions	Far superior in terms of accuracy, consistency and/or timeliness of predictions
Higher scores are more advantageous to Continuous Monitoring						

The following six tables present the detailed results for these questions for the three scenarios.

Table 6.22 Digital Data Distribution by Likert Scale

	1	2	3	4	5	Total Vote	# of No Judgments
Sony	0%	25%	16%	44%	15%	237	13
Bear Stearns	7%	39%	11%	38%	5%	180	20
Blackberry	15%	26%	9%	34%	15%	163	28
Total	**7%**	**30%**	**13%**	**39%**	**12%**	**580**	**61**

Table 6.23 Cost Human Judgment Distribution by Likert Scale

	1	2	3	4	5	Total Vote	# of No Judgments
Sony	0%	7%	39%	40%	13%	241	14
Bear Stearns	3%	7%	39%	44%	7%	203	22
Blackberry	2%	15%	49%	26%	8%	171	28
Total	**2%**	**9%**	**42%**	**37%**	**9%**	**615**	**64**

Table 6.24 Cost Predictive Model Distribution by Likert Scale

	1	2	3	4	5	Total Vote	# of No Judgments
Sony	7%	59%	30%	4%	0%	164	10
Bear Stearns	9%	42%	39%	8%	2%	165	15
Blackberry	13%	30%	41%	13%	4%	143	27
Total	**9%**	**45%**	**36%**	**8%**	**2%**	**472**	**52**

Table 6.25 Human Judgment Detect Risk Distribution by Likert Scale

	1	2	3	4	5	Total Vote	# of No Judgments
Sony	7%	27%	39%	21%	6%	207	10
Bear Stearns	14%	22%	28%	25%	12%	195	16
Blackberry	15%	27%	28%	23%	7%	168	21
Total	**12%**	**25%**	**32%**	**23%**	**8%**	**570**	**47**

Table 6.26 Predictive Model Can be Built Distribution by Likert Scale

	1	2	3	4	5	Total Vote	# of No Judgments
Sony	1%	12%	28%	46%	13%	243	13
Bear Stearns	8%	23%	28%	27%	14%	202	17
Blackberry	13%	20%	22%	33%	11%	167	27
Total	**7%**	**18%**	**26%**	**35%**	**13%**	**612**	**57**

Table 6.27 Model compared to Human Judgment Distribution by Likert Scale

	1	2	3	4	5	Total Vote	# of No Judgments
Sony	3%	10%	24%	49%	14%	253	11
Bear Stearns	8%	11%	32%	33%	16%	213	18
Blackberry	14%	21%	32%	23%	9%	163	25
Total	**8%**	**14%**	**29%**	**36%**	**13%**	**629**	**54**

The "Ryan-Joiner" Normality Test concluded that the variables are normally distributed at an $\alpha = 0.05$ ($p=0.07$). In aggregate, the results of Round 2 mirrored Round 1. Averaging each case's six question Likert score, respondents in Round 2 ranked Sony as the most advantageous Continuous Monitoring scenario with a mean Likert score of 3.24 out of 5, which was followed by Bear Stearns with a mean Likert score of 3.06 out of 5, while RIM was viewed as the least advantageous scenario with a mean Likert score of 2.95 out of 5 (see below table).

Table 6.28 Mean Likert Scaled Values by Question

Factors	Sony	Bear Stearns	RIM	Total
Cost Human Judgment	3.60	3.44	3.23	3.44
Cost Predictive Model	2.31	2.50	2.65	2.47
Digital Data	3.49	2.95	3.08	3.19
Human Judgment Detect Risk	2.92	3.00	2.80	2.91
Predictive Model Can be Built	3.57	3.16	3.09	3.29
Predictive Model compared to Human	3.61	3.38	2.91	3.33
Mean Likert Score	**3.24**	**3.06**	**2.95**	**3.10**
"No Judgment" responses were excluded from mean calculations				

A one-way ANOVA was calculated between the three scenarios across all six factors. The variance between scenarios was significant at an $\alpha = 0.05$ ($p = .00$). Therefore, participants viewed some scenarios as more advantageous to Continuous Monitoring than other scenarios. Specifically, the Sony scenario that dealt with risk of computer crime was viewed as a more promising Continuous Monitoring endeavor than

the operational and strategic risks illustrated by the Bear Stearns and RIM scenario respectively. This ranking is consistent with the ranking identified in Round 1 (see Subsection 6.1.7).

6.2.2 RQ3: Requisite Architectural Components

Research Question 3 seeks to determine the requisite Continuous Monitoring architectural components and determine the ones that are most applicable to an Enterprise Risk. In questions 9, 16 and 23 of Round 2 participants were asked to select all the components that they believed would be in a Continuous Monitoring system for the Sony, Bear Stern, and RIM scenarios respectively. Generally speaking, the participants were roughly evenly divided on whether or not a component was needed for each scenario. Table 6.29 summarizes the percentage of participants that selected each component across the three scenarios.

Table 6.29 Percentage of Participants that stated a Component was Needed

	Analytical Functions	**Dashboard Reporting**	**Data Warehouse**	**Digital Agents**	**Workflow**
Bear Stearns	49%	53%	54%	49%	43%
RIM	58%	47%	46%	42%	32%
Sony	48%	49%	52%	63%	49%

A Kruskal-Wallis test was run on the five components; Analytic Functions, Dashboard Reporting, Data Warehouse, and Digital Agents and Workflows, which were described in Chapter 4. This test indicated that Digital Agents and Workflows were used differently across the three business scenarios. Moreover, there was no usage difference among the other three components (i.e., Analytical Functions, Dashboard Reporting and Data Warehouse) at an $\alpha = 0.05$. See the below table.

Table 6.30 Mean Likert Scaled Value by Question

Component	Sony Median	Bear Stearns Median	RIM Median	P-Val Adjusted for ties
Digital Agents*	1	0	0	0.03
Workflows**	0	0	0	0.08
Analytical Functions	0	0	1	0.39
Data Warehouse	1	1	0	0.53
Dashboard Reporting	0	1	0	0.73
Scale 1 = Use the Component, 0 = Don't use the Component * Significant at α = 0.05 ** Significant at α = 0.10				

Participants were also asked to suggest other potential architectural components for each business scenario. A qualitative review of their responses uncovered no new architectural components, which offers strong evidence that the literature review identified the main architectural components for a Continuous Monitoring system.

6.3 Round 3

Research Question 4 measures how participation in this research study changes the initial viewpoints of the participants. The Round 3 survey was hosted by Surveymonkey.com and was open from January 24, 2015 to February 7, 2015. Round 3 had 59 respondents that completed the entire survey. The between round dropout rate was 27%. The complete set of questions is listed in Appendix C. On balance participants feel they obtained useful information from this research study (i.e., the mean Likert score for Question 21 was 2.6); this was a high quality research study (i.e., the mean Likert score for Question 24 was 4.2); and its results have the potential to be important (i.e., the mean Likert score for Question 22 was 2.7)

6.3.1 RQ4: Research Study Changes Viewpoints

Research Question 4 measures how participation in this research study changes the initial viewpoints of the participants. In Round 1 and 3, the participants were asked, "To what extent do you believe that Continuous Monitoring has the potential to provide material business value to today's companies?" The Likert score scale was

5 - Very Likely
4 – Likely
3 – Neutral
2 – Unlikely
1 – Very Unlikely

Table 6.31 has the distribution of responses to these questions. Those that answered, "I don't know" were excluded from this analysis.

Table 6.31 Continuous Monitoring Value Proposition Distribution Round 1 and 3

	Round 1		**Round 3**	
Responses	**#**	**%**	**#**	**%**
Very likely	73	40%	17	29%
Likely	83	45%	34	58%
Neutral	26	14%	4	7%
Unlikely	0	0%	3	5%
Very unlikely	2	1%	1	2%
Total	**184**	**100%**	**59**	**100%**

For this question, the mean Likert response in Round 1 was 4.22 and in Round 3 it was 4.07. Therefore, the perceived business value of Continuous Monitoring dropped slightly between Rounds 1 and 3. One possible explanation for this decrease is that as participants pondered the complexities of a Continuous Monitoring system within the context of a specific business case, the implementation complexities caused their optimism to dip.

The Ryan-Joiner normality had a p-value of 0.01, which implies that this variable was not normally distributed at $\alpha = 0.05$. As a result, the Kruskal-Wallis test was used to determine if this question's decrease between Round 1 and Round 3 was significant. The resulting p-value was 0.30. Therefore, this decrease was not significant at an $\alpha = 0.10$, which implies that participating in this study did not significantly affect participant's perceptions of Continuous Monitoring's business value.

In Round 2 there was a non-trivial amount of standard deviation, which represents disagreement between the respondents about the viability of Continuous Monitoring. In an attempt to drive consensus among participants, Round 2's assumptions questions (see Questions 4, 6, 7, 8, 11, 13, 14, 15, 18, 20, 21 and 22 in Appendix B) were qualitatively analyzed and the most frequently listed assumptions were voted on in Round 3 (see Questions 3, 9 and 15 in Appendix C for a complete lists of assumptions). Every question in Round 3 had a lower standard deviation than the corresponding question in Round 2.

Table 6.32 Standard Deviation by Question between Rounds

Question	Case	Round 2	Round 3
Cost Human Judgment	Bear Stearns	1.7	1.0
	RIM	1.7	1.2
	Sony	1.6	1.0
Cost Predictive Model	Bear Stearns	1.2	1.0
	RIM	1.5	1.2
	Sony	1.0	0.8
Predictive Model Can be Built	Bear Stearns	1.7	1.0
	RIM	1.8	1.2
	Sony	1.6	1.1
Model Compared to Human Judgment	Bear Stearns	1.7	1.1
	RIM	1.7	1.4
	Sony	1.5	1.2

Since a Ryan-Joiner normality test implied that the these questions were generally not normally distributed at $\alpha = 0.05$, a Kruskal-Wallis Test was used to compare Round 1 and Round 3 results. Bear Stearns and Sony's "Cost of Human Judgment" question, RIM and Sony's "Cost of Predictive Model" question, and RIM's "Predictive Model Can be Built" question and "Predictive Model Compared to Human Judgment" question all had significant changes between Rounds 2 and 3. See below table.

Table 6.33 Median by Question between Rounds

Question	Case	Median Round 2	Median Round 3	P-Value
Cost Human Judgment	Bear Stearns*	3	2	0.03
	RIM	3	2	0.75
	Sony*	3	2	0.00
Cost Predictive Model	Bear Stearns	2	2	0.31
	RIM**	2	2	0.02
	Sony**	2	2	0.07
Predictive Model Can be Built	Bear Stearns	3	3	0.58
	RIM*	2	3	0.07
	Sony	3	3	0.36
Model Compared to Human Judgment	Bear Stearns	3	3	0.11
	RIM**	2	3	0.02
	Sony	4	4	0.72

* Significant at $\alpha = 0.05$
** Significant at $\alpha = 0.10$

In conclusion the Delphi appears to have driven consensus between participants as evidenced by the lower standard deviation between rounds. However another possible explanation for the decrease in standard deviation is that 22 participants dropped out of the research experiment between Rounds 1 and 2. Perhaps, the participants that completed Round 3 were more likeminded than those who dropped out.

6.4 Limitations

This research study suffers from the limitations of all self-reported studies. Specifically, respondents may provide answers that they believe the researcher wants to hear, forget pertinent details, provide exaggerated or incorrect answers, and/or may not reveal overly private information. Moreover, participants may have various biases, perception limitations and/or gaps in their understanding that skew their answers. In this research study many questions' most frequently selected answer was "I don't know", which may indicate that several participants had gaps in their understanding of the requisite domain.

Secondly, there could be a self-selection bias between the respondents, who participated in this research study and those who did not. If there is a systematic difference between these groups, it could bias the results. Similarly, the between round dropout rate was high, which could also bias the results between those that completed the later rounds and those that did not. The high dropout rate may have resulted from the lengthy and intricate surveys. This maybe an inherent limitation of the survey research method. Perhaps, a better research approach would have been to use shorter surveys or maybe even another research method such as focus groups.

Thirdly, the response rate for those working at Big 4 accounting firms was particularly low, which could have biased the results of Research Question 1. Research Question 1 tested the relationship between working at a Big 4 accounting firm and the perceived Business Value of Continuous Monitoring. Perhaps if more Big 4 accountants had participated in this research, this hypothesis would have been supported.

Finally, this study only evaluated a limited number of scenarios. In all, only three business cases for three Enterprise Risks were studied. There is a risk that the selected

business cases were not representative of the underlying Enterprise Risk, which could have skewed the results. Moreover, there were many Enterprise Risks that were not included in this research experiment. Perhaps including these Enterprise Risks would have yielded different results.

CHAPTER 7

CONCLUSION

Whether or not Continuous Monitoring could be meaningfully extended to Enterprise Risks still remains an open research question. The obstacles to building such a system are formidable. Replacing human judgment tends to be difficult, costly and computationally intensive. Moreover, large-scale Continuous Monitoring systems may be resisted because of their inscrutable complexity and novelty. However, many believe that Continuous Monitoring systems will lead to a more robust and effective organizational risk management structure.

In the future, Continuous Monitoring could be the cornerstone of risk management programs. Initially these systems were designed to remove fraud and other similar pathogens from the organization. Perhaps the absence of fraud and other similar dysfunctions is not the pinnacle of a healthy organization and just like organisms, organizations may require more than the absence of pathogens to be completely "healthy".

Perhaps, Continuous Monitoring systems could provide a useful check on human decision-making. Advances in artificial intelligence, big data and Information Systems may lead to new classes of decision verification systems that will help improve organization decision-making, which could not only increase profitability, but also reduce the probability of the next financial crisis. There is still much more research that is needed in order to make this possibility a reality.

7.1 Contributions

As a direct result of this research study, a new key relationship was identified between perceived business value of Continuous Monitoring and the number of years of experience in Risk Management and Auditing. Participants that had more than five years of experience in either discipline tended to view Continuous Monitoring more positively than participants that had less than five years of experience. This relationship was statistically significant in both Round 1's exploratory data analysis and the factor analysis for the Feasibility and Desirability questions, which were Question 15 and Question 16 respectively.

Secondly, this research identifies preferred Enterprise Risks for Continuous Monitoring systems. Participants were more optimistic about Continuous Monitoring Systems' ability to handle computer crime situations than their ability to navigate strategic issues such as a company losing its competitive position. Moreover, this research identified three novel uses for Continuous Monitoring: 1) monitoring social media to detect potential reputational risks and/or looming public relations crises. 2) monitoring the speed of operational and production processes. 3) monitoring medical records for potential early warning signs of a serious medical condition.

Thirdly, this research provides a wealth of qualitative information that could be used in other studies. For example, the specific risk scenarios gathered by this research could form the basis of a future Cross Impact Assessment (Bañuls and Turoff 2011). Finally, this research provides another illustrative example of the Delphi method driving consensus among research participants.

7.2 Future Research

This research study provides a general approach for understanding whether Continuous Monitoring is applicable to an Enterprise Risk. This research study only covered three of the 14 identified Enterprise Risks. Future research studies can use the same methodology to study these other Enterprise Risks as well as any new types of Enterprise Risk that arise. The same methodology could be adapted to study how Continuous Monitoring could be adapted to a specific industry's most pressing Enterprise Risks.

Moreover this literature review uncovered many broad categories of research needed to advance Continuous Monitoring. The list below is the ten most important questions that I believe should be researched.

1. Workflow: What heuristics could be used to manage and/or prioritize exceptions identified by a Continuous Monitoring system? How should Continuous Monitoring workflow be configured? Who should be notified when an exception is identified and how often?
2. Data: Determine what forms of financial, non-financial, competitive, marketing and/or qualitative assurance information should be used in a Continuous Monitoring system. Identify and analyze potential difficulties associated with the evaluation of data and overcoming data gaps.
3. Data Analysis Algorithms: Can artificial intelligence techniques be used to improve Continuous Monitoring strategies? How are the monitoring rules stored and applied to the continuous data stream?
4. Improving Thoroughness and Reliability of decision-making: Empirically test the relationship between Continuous Monitoring and Organizational decision making. Does Continuous Monitoring hasten the detection of errors and decrease the number of bad decisions made by corporations?
5. NPV and Break Even point for a Continuous Monitoring system: Investigate the extent to which the initial development and deployment costs of Continuous Monitoring systems can be offset by ongoing savings.
6. Behavioral Effects: Investigate whether managers, analysts and/or markets will exhibit an adverse or positive reaction to Continuous Monitoring. How will constituents interact and integrate with Continuous Monitoring systems?

7. Architectural Framework: What is the ideal architecture to integrate control frameworks that link together entities, processes, metrics, analytics and alarms? Are there systematic differences in the architecture between Continuous Monitoring implementations? If so what drives them (e.g., industry, size, IT characteristics, external auditor, supply partner integration, or international presence)?
8. Security Issues: Examine the extent to which a Continuous Monitoring system will create security vulnerabilities. How can the Continuous Monitoring data be secured? How can data tampering be prevented? What are the requisite safeguards to ensure the system is not gamed?
9. Success Factors: What are the organizational factors that lead an organization to adopt Continuous Monitoring technologies?
10. How to audit the decision-maker: For most risks, human judgment is needed. How can Information Technology audit decisions made by humans? Many complex business decisions have conflicting criteria and require tradeoffs between competing objectives. Is it even possible to automate the monitoring of these decisions? If so, how could the requisite decision data be captured and analyzed?

APPENDIX A

ROUND 1 PRE-SURVEY AND SCENARIO GENERATION

This survey was implemented on Survey Monkey:

Introduction to Robert Baksa's Research Study

ABOUT THIS STUDY:
This is a study of business managers' opinions about the potential usefulness of Continuous Monitoring to manage Enterprise Risks. Participation in this study typically takes less than an hour for each of its three rounds. Participants begin by filling in a formal consent form and providing some background information. In the subsequent, two rounds a series of targeted questions will be presented. Many individuals find participation in this study enjoyable, as well as informative. It will give you the opportunity to engage in sharing opinions and discussions with your peers in other companies.

ABSTRACT:
A constantly evolving regulatory environment, increasing market pressure to improve operations, and rapidly changing business conditions are creating the need for timely and ongoing assurance that organizational risks are continually and adequately identified and mitigated. Enterprises are perpetually exposed to significant errors, fraud and/or inefficiencies that can lead to significant financial loss and increased levels of operating risk. Increasingly Information Systems are being harnessed to reinvent the risk management process. One promising technology is Continuous Auditing, which seeks to transform the audit process from periodic reviews of a few transactions to a continuous review of all transactions. However, today's highly integrated, rapidly changing and hypercompetitive business environment spawns numerous risks that have been excluded from standard risk management and planning processes. An extension of Continuous Auditing is Continuous Monitoring, which is used by management to continually review business processes for unexpected deviations. Many believe that Continuous Monitoring systems will lead to a more robust and effective organizational risk management processes.

ABOUT ME:
I am a seasoned Information Systems executive with over two decades of technical, financial, implementation, consulting and risk management expertise, as well as a proven track record for delivering complex Information Technology systems that produce tangible financial results. Some of the more notable projects that I've led include reengineering GM's financial control systems, developing Citi's award-winning foreign exchange trading system, and building Kaplan's next generation eLearning platform. In addition, I authored Chapter 12 of Supporting Real Time Decision-Making: The role of Context in Decision Support on the Move. I have an MBA from the Stern School of

Business, a Master of Science in Information Systems from New York University, and a Bachelor of Science in Computer Science and Business from the University of Pittsburgh. Currently, I am a Ph.D. candidate in Information Systems at New Jersey Institute of Technology and employed as a Delivery Practice Head for Lab49, which is a design and technology-consulting firm that creates advanced technology solutions for the world's leading investment banks, asset managers and exchanges

WEBBOARD:
If you would like to interact with your fellow research participants, please go to my WebBoard http://baksaphd.activeboard.com/ at any point during this research study. After you complete this survey, go to this web board and click the "Register" link. However, even without an account, you can browse the posted material and post an anonymous message to the group.

REFER A FRIEND:
The ideal research participant will be over 21 years of age and have at least five years of professional experience with operational risk management, Information Systems and/or auditing. If you know someone that fits this profile and would be potentially willing. Please contact the researcher.

1. Please Enter Your Full Name (i.e., First and Last).

2. Please enter your preferred email address.

CONSENT
NEW JERSEY INSTITUTE OF TECHNOLOGY
323 MARTIN LUTHER KING BLVD.
NEWARK, NJ 07102

TITLE OF STUDY:
Continuous Monitoring of Enterprise Risks: a Delphi Feasibility Study.

DURATION:
Maximum estimated duration is 6 months, which assumes two months per round for the three scheduled rounds.

RESEARCH STUDY:
I have been asked to participate in a research study under the direction of Drs. Murray Turoff and Starr Roxanne Hiltz.

PROCEDURES:
During the course of this study, I will participate in on-line Delphi surveys and potentially share my thoughts on a message board.

PARTICIPANTS:
I will be one of no more than 80 participants in this study.

EXCLUSIONS:
There are two mandatory requirements for this research study: 1) Participants must be over the age of 21. 2) Participants must have at least five years of professional experience with risk management, Information Systems and/or auditing. I will inform the researcher if I do not satisfy the aforementioned requirements.

RISKS/DISCOMFORTS:
I have been told that the study described above involves no obvious risks and/or discomforts. However, there may be risks and discomforts that are not yet known. I fully recognize that there may be risks that I may be exposed to by volunteering in this study which are inherent in participating in any study; I understand that I am not covered by NJIT's insurance policy for any injury or loss I might sustain in the course of participating in the study.

CONFIDENTIALITY:
I understand confidentiality is not the same as anonymous. In this context, confidentiality means that my name or affiliation will not be disclosed, without expressed permission. Reasonable safeguards will be put in place to protect participant's confidentiality. The raw research data, including the survey responses will be stored on the researcher's password-protected and encrypted computer. Moreover, if the findings from the study are published, participants that don't grant consent will not be identified by name in the list of participants and their responses, if used, will not be associated with a named individual. If there is a documented linkage between their identity and responses, reasonable efforts will be made to maintain their confidentiality unless disclosure is required by law.

PAYMENT FOR PARTICIPATION:
I have been told that I will receive no compensation for my participation in this study.

RIGHT TO REFUSE OR WITHDRAW:
I understand that my participation is voluntary and I may refuse to participate, or may discontinue my participation at any time with no adverse consequence. I also understand that the investigator has the right to withdraw me from the study at any time.

INDIVIDUAL TO CONTACT:
If you have any questions about the survey's questions, please browse the FAQ thread of the WebBoard: http://baksaphd.activeboard.com/ or contact the researcher directly:
Robert Baksa

If I have any questions about my treatment or research procedures, I understand that I should contact the principal investigator at:
Murray Turoff
Roxanne Hiltz

If I have any additional questions about my rights as a research subject, I may contact:
Judith Sheft, IRB Chair, New Jersey Institute of Technology

CONSENT OF PARTICIPANT

I have read this entire form, and I understand it completely. By "Yes" below, I acknowledge that I have read this information and agree to participate in this research, with the knowledge that I am free to withdraw my participation at any time without penalty.

3. I willingly consent to participate in this research study?
   - Yes
   - No

4. What is your age?
   - Less than 21 years old
   - 21-34 years old
   - 35-44 years old
   - 45-54 years old
   - 55-64 years old
   - 65-74 years old
   - 75 years or older
   - Prefer not to answer

5. How many years of professional experience do you have in the following areas? Enter 0 if you have no experience in a particular area.
   - Risk Management
   - Information Systems
   - Internal and/or External Auditing

6. Can we use your name in a list of participants in the research results? (If no, "anonymous" will be substituted for your name)?
   - Yes
   - No

7. What is your gender?
   - Female
   - Male
   - Prefer NOT to answer

8. What is the highest level of education that you have completed?
   - High School
   - Bachelors
   - Masters
   - Doctorate
   - None of the above

9. In what industry do you currently work?
   - Healthcare

Manufacturing
Education
Banking/Finance
Insurance
Communications
Transportation
Government
Retail
Hospitality
Other
Not Currently Employed

10. Are you employed by either PWC, Deloitte & Touche, Ernst & Young and/or KPMG?
Yes
No

11. How large is your current employer in terms of Total Annual Revenue?
Under $1M
> $1 Million and <= $10 Million
> $10 Million and <= $100 Million
> $100 Million <= $500 Million
> $500 Million <= $1 Billion
Over $1 Billion
Not sure / Don't know

12. What is your current role in the organization?
C-Level Executive (i.e., CEO, CTO, CIO etc.)
Senior Management (i.e., responsible 50+ people, a geographic region, or product)
Supervisor / Middle management (i.e., has less than 50 direct reports)
Not Employed
Other

13. To what extent do you believe that Continuous Monitoring has the potential to provide material business value to today's companies?
Very Likely
Likely
Neither Likely or Unlikely
Unlikely
Very Unlikely
Don't Know

14. In general how feasible would building a Continuous Monitoring system be for this category of risks

	Very feasible	Feasible	Possibly feasible	Unfeasible	Very Unfeasible	Don't Know
a) Economic Volatility or Slowdown: Another major financial crisis (e.g., Mortgage default) and/or downturn. Recent examples include weakness in the Eurozone, projected slowed economic growth forecast in India and China, persistent fiscal changes in Japan, and elevated worldwide unemployment rate, reoccurring financial crisis, failure of major countries to pay their debt						
b) Regulatory pressure and/or changes in regulatory environment: Basel III, SOX, Dodd-Frank, Solvency II, foreign corrupt practices legislation, local privacy, investigation by government agency or regulatory body & laws and the International Financial Reporting Standards, Health Care reforms						
c) Surprise Competitive Threats: New and, perhaps better, competitors and/or products in the marketplace change in consumer trends and technological advancements (i.e., product obsolesces), increased global competitive pressures, aggressive competitive tactics (such as price wars), mergers and acquisitions.						
d) Credit, Market and Liquidity Risk						
e) Damage to brand/reputation: product recalls, regulatory challenges (e.g., JP Morgan Chase), involvement in a corporate or personal scandal (e.g., Martha Stewart), failure of core strategy or product (e.g., Blackberry), unable to meet demand for successful product, being flamed on social media.						
f) Legal Risks: Customer and employee lawsuits						
g) External Business interruption: Infrastructure failures (e.g., electricity and telecommunication network failures), financial market failures (closing of key markets), loss of computer infrastructure, transportation strikes, criminal attacks, or embargos.						
h) Internal Business interruption: For example strike or slowdown, accidents, fraud, workplace violence, industrial accidents (e.g., nuclear power plant explosion of materials or fires).						
i) Commodity Price Risk: Crude oil, Natural gas, shortages that lead to price run-ups.						
j) Computer Crime: Financial losses from virus and malicious code, proprietary or customer information can be stolen via hacking or internal theft (e.g., target customer credit cards); malicious software can disrupt operations of essential services such as security, defense, power plants, as well as banking, commerce, etc.						

15. How desirable would building a Continuous Monitoring system be for this category of risks?

	Very Desirable	Desirable	Neither Desirable nor undesirable	Undesirable	Very Desirable	Don't Know
a) Economic Volatility or Slowdown: Another major financial crisis (e.g., Mortgage default) and/or downturn. Recent examples include weakness in the Eurozone, projected slowed economic growth forecast in India and China, persistent fiscal changes in Japan, and elevated worldwide unemployment rate, reoccurring financial crisis, failure of major countries to pay their debt						
b) Regulatory pressure and/or changes in regulatory environment: Basel III, SOX, Dodd-Frank, Solvency II, foreign corrupt practices legislation, local privacy, investigation by government agency or regulatory body & laws and the International Financial Reporting Standards, Health Care reforms						
c) Surprise Competitive Threats: New and, perhaps better, competitors and/or products in the marketplace change in consumer trends and technological advancements (i.e., product obsolesces), increased global competitive pressures, aggressive competitive tactics (such as price wars), mergers and acquisitions.						
d) Credit, Market and Liquidity Risk						
e) Damage to brand/reputation: product recalls, regulatory challenges (e.g., JP Morgan Chase), involvement in a corporate or personal scandal (e.g., Martha Stewart), failure of core strategy or product (e.g., Blackberry), unable to meet demand for successful product, being flamed on social media.						
f) Legal Risks: Customer and employee lawsuits						
g) External Business interruption: Infrastructure failures (e.g., electricity and telecommunication network failures), financial market failures (closing of key markets), loss of computer infrastructure, transportation strikes, criminal attacks, or embargos.						
h) Internal Business interruption: For example strike or slowdown, accidents, fraud, workplace violence, industrial accidents (e.g., nuclear power plant explosion of materials or fires).						
i) Commodity Price Risk: Crude oil, Natural gas, shortages that lead to price run-ups.						
j) Computer Crime: Financial losses from virus and malicious code, proprietary or customer information can be stolen via hacking or internal theft (e.g., target customer credit cards); malicious software can disrupt operations of essential services such as security, defense, power plants, as well as banking, commerce, etc.						

16. Describe a specific risk scenario that you feel would be the most auspicious area for a Continuous Monitoring system. Ideally this risk scenario would NOT already be adequately mitigated by the operating controls currently in place and would be achievable with existing technology. Please briefly suggest leading indicators, potential consequences of this risk, and plausible mitigation options. (Optional Question)

APPENDIX B

ROUND 2: DELPHI

This survey was implemented on Survey Monkey:

Summary of Round 2 Results:

In Round 1, there were 188 fully completed responses, 29 of which were from C-Level executives (e.g., CEOs, CTOs CIOs, etc.). Respondents had an average of 13 years of I.T. experience, and six years of risk management and internal/external audit experience. 122 respondents (65% of the total) identified themselves as male and only 11 (6% of the total) have worked at a Big 4 accounting firm.

The respondents worked in a multitude of different industries. In fact, 60% selected "Other" for their industry and of the ten industries listed on the survey; each had three or more respondents. The respondents tended to work in larger companies. "Over a billion", which was the largest revenue category on the survey, and was also the most frequently selected, with 50 respondents (27% of the total). The other 5 revenue levels all had at least ten respondents each.

Overall, the respondents had a very positive view of Continuous Monitoring. 73 respondents (39% of the total) believed Continuous Monitoring is "Very Likely" to have material business value, while 83 respondents (44% of the total) believe Continuous Monitoring is "Likely" to have material business value. In terms of feasibility and desirability, the top three Enterprise Risks that the participants felt lend themselves to a Continuous Monitoring system are: (1) Computer Crime (2) Credit, Market and Liquidity Risk (3) Damage to Brand and Reputation. More respondents (33 or 17.5% of the total) suggested a specific computer crime scenario (e.g., hacking, IP theft, etc.) as the most auspicious area for a Continuous Monitoring system. Figure 1 below has the detailed breakdown of the results.

1. Please Enter Your Full Name (i.e., First and Last)

2. Please enter your preferred email address?

Directions for Round 2

This round will focus on the top three Enterprise Risks identified in the prior round. Please read carefully the following excerpts from three Harvard Business School Cases that describe a specific example of a type of Enterprise Risk and answer the questions that follow. By design, these cases describe real events that were heavily covered by the media. So please feel free to pull in additional information that isn't explicitly stated.

If you have questions about this round or would like to interact more with your fellow research participants, please go to my WebBoard: http://baksaphd.activeboard.com/. Alternatively, you can email your questions directly to me at rbb25@njit.edu

Sony PlayStation: Security Breach
by (Seijts and Bigus 2012) HBS: W12309

Launched by Sony in 2010, Qriocity provided a cloud-based digital video and music service to consumers. Operated as a subscription service, Qriocity users set up an online account and paid a fee to access content. For Sony, Qriocity represented an opportunity to better integrate the company's consumer electronics with online music, movies and games. In 2011, Sony had over 350 million Internet-connected devices in use around the world, providing the company with a significant market of potential Qriocity customers.

Sometime between Sunday, April 17 and Tuesday, April 19, 2011, Sony's PlayStation and Qriocity user account information had been compromised as the result of an illegal intrusion into the company network. In response to this security threat, on Wednesday, April 20, 2011, Sony suspended all PlayStation and Qriocity networks services for 24 days, while Sony retained an external security firm to conduct a complete investigation of the incident. On May 4, Sony confirmed that personal information including names, birthdates, physical and e-mail addresses, network IDs and passwords, and possibly credit card information was stolen from its 77 million customers, which makes it one of the largest data security breaches in history. On May 23, Sony stated that this outage cost $171 million.

Sony had several security incidences before the attack. First, a month before the attack, the PlayStation.com website was a hacked by a group called Anonymous, apparently in response to Sony taking legal action against two modders, who are hackers that modify their consoles to give them additional functionality. Second, PlayStation 3 modders were claiming that PSN Web servers were running outdated versions of Apache and Linux, which had well known vulnerabilities. Finally, two weeks before the intrusion, Sony's networks were probed by a program that checks for known security vulnerabilities. Some speculate that if Sony had used an intrusion detection system prior to the attack, they may have noticed these vulnerabilities, which may have prompted them to heighten their defenses to guard against an attack.

Sony submitted written answers to questions posed by the United States House Subcommittee about this cyber-attack. Sony stated that they were the victim of a very carefully planned, professional, highly sophisticated criminal cyber-attack. The forensic teams were able to confirm the scope of the personal data they believed had been taken, and could not rule out that credit card information was also taken. They were taking a number of steps to prevent future breaches.

For this type of cyber-attack risk scenario, please answer the following questions:

3. Can the data required to understand the current degree of this type of risk be obtained from current digital sources (e.g., databases or online sources, etc.)? (Ignore costs of access).

No Judgment / I don't know
None or very little of the data needed is in a digital form
Some of the relevant data is available digitally
About half of the relevant data is available digitally
Most of the relevant data is available digitally
All the relevant data is available digitally

4. Can a real time predictive model be constructed with a reasonable effort and investment within a one-year time horizon by an appropriate development group?

No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

Please list at least one assumption that you made about the use of data sources in a predictive model including any specific data related challenges related to integrating the data into the model.

5. Would reliance on human judgments (i.e., either internal expertise or professional consultants) be able to adequately detect changes in the degree of this risk?

No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

6. Relative to conventional human judgment, a real-time predictive model would be

No Judgment / I don't know
Far inferior in terms of accuracy, consistency and/or timeliness of predictions
Moderately inferior in terms of accuracy, consistency and/or timeliness of predictions
About the same
Moderately superior in terms of accuracy, consistency and/or timeliness of predictions
Far superior in terms of accuracy, consistency and/or timeliness of predictions

Please list at least one relevant assumption that you made in regards to this question.

7. The cost of building a real-time predictive model for this risk would be:
No Judgment / I don't know
Extremely cheap
Relatively cheap
Reasonable
Moderately expensive
Prohibitively expensive

Please list at least one relevant assumption that you made about the cost of building this real-time predictive model.

8. The costs of relying on human judgments (i.e., either internal expertise or professional consultants) for this risk would be:
No Judgment / I don't know
Prohibitively expensive
Moderately expensive
Reasonable
Relatively cheap
Extremely cheap

Please list at least one relevant assumption that you made about reliance on human judgments.

9. Select all the components that would likely be contained in a Continuous Monitoring system for this type of risk (check all that apply). Leave this question blank if you believe none of the below are required or you don't have an opinion.
Analytical Functions (e.g., Regression Models, Expert Systems, Neural Nets, etc.)
Dashboard Reporting
Data Warehouse
Digital Agents (e.g., software that autonomously performs services or collects data)
Workflows (i.e., orchestrated and repeatable pattern of business activity supported by a systematic process)
Other (please specify)

Bear Stearns
by (Rose, Bergstresser et al. 2009)

Founded in 1923, Bear Stearns & Co. (Bear) was the fifth largest U.S. investment bank in early 2008. However, it burned through nearly all of its $18 billion in cash reserves during the week of March 10, 2008. Bear's economic engine was its fixed income business. In 2006, Bear's fixed income business contributed $3.62 billion in revenues, compared to $1.33 billion from investment banking and $1.38 billion from equities. Mortgages and mortgage-backed securities comprised most of the fixed income business, representing about 31% of the securities it owned. Bear was among the largest players in the mortgage market, and was the leading underwriter of U.S. mortgage backed securities from 2004 to 2007.

New financial market stresses, largely rooted in the U.S. housing market, emerged in 2007 and intensified in early 2008. Because home mortgages and home equity loans were frequently packaged and sold in securities that were in turn sold to a wide variety of investors, the rapid deterioration of housing prices was widely felt and created a heightened sense of anxiety across the financial markets. U.S. housing prices had appreciated rapidly between 1998 and 2006. This occurred alongside easier access to mortgage finance, especially among less credit-worthy borrowers. The origination of subprime mortgage loans grew from $190 billion in 2001 to $625 billion in 2005.

Even during auspicious periods, mortgage backed securities were often illiquid. As default rates rose and macroeconomic conditions deteriorated, the absence of a liquid trading market forced investors to seek bids from the commercial and investment banks that initially created and sold them. Wary of repurchasing too much of these securities, banks began to reduce the price they would pay and quantity they would buy for these securities. This only increased the downward pressure on bond prices, creating a "vicious circle" among the holders of mortgage backed securities: in addition to the uncertainty in fundamental value created by rising default rates, the reduction in prices by the bond dealers created even greater urgency on the part of investors to sell these securities, which forced the dealers to mark prices down even further. This vicious circle caused dealers, such as Bear, to accumulate larger and larger inventories of these securities, which were valued at perpetually lower prices.

Two large hedge funds managed by Bear Stearns had invested heavily in illiquid Collateralized Debt Obligations tied to mortgage backed securities. These funds had magnified their exposure to mortgage markets through the use of leverage; the fund managers were able to purchase as much as $60 worth of Collateralized Debt Obligations for each dollar invested. When these funds began selling assets to meet investor demands, it quickly led to the implosion of Bear. Bear survived to the close of business on Friday, March 14 only because of that morning's groundbreaking announcement: the Federal Reserve Bank of New York (N.Y. Fed), using JP Morgan Chase & Co. (JPMC) as a conduit, would provide Bear with secured financing for a period of up to 28 days. Despite this unprecedented provision of liquidity support, it was insufficient to reverse the decline in Bear's condition. On March 16, Bear's board accepted JPMC's offer to purchase Bear for $2 per share, which was subsequently increased to $10 a share.

For this type of liquidity risk scenario, please answer the following questions:

10. Can the data required to understand the current degree of this type of risk be obtained from current digital sources (e.g., databases or online sources, etc.)? (Ignore costs of access).

No Judgment / I don't know
None or very little of the data needed is in a digital form
Some of the relevant data is available digitally
About half of the relevant data is available digitally
Most of the relevant data is available digitally
All the relevant data is available digitally

11. Can a real time predictive model be constructed with a reasonable effort and investment within a one-year time horizon by an appropriate development group?

No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

Please list at least one assumption that you made about the use of data sources in a predictive model including any specific data related challenges related to integrating the data into the model.

12. Would reliance on human judgments (i.e., either internal expertise or professional consultants) be able to adequately detect changes in the degree of this risk?

No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

13. Relative to conventional human judgment, a real-time predictive model would be

No Judgment / I don't know
Far inferior in terms of accuracy, consistency and/or timeliness of predictions
Moderately inferior in terms of accuracy, consistency and/or timeliness of predictions
About the same
Moderately superior in terms of accuracy, consistency and/or timeliness of predictions
Far superior in terms of accuracy, consistency and/or timeliness of predictions

Please list at least one relevant assumption that you made in regards to this question

14. The cost of building a real-time predictive model for this risk would be:
No Judgment / I don't know
Extremely cheap
Relatively cheap
Reasonable
Moderately expensive
Prohibitively expensive

Please list at least one relevant assumption that you made about the cost of building this real-time predictive model.

15. The costs of relying on human judgments (i.e., either internal expertise or professional consultants) for this risk would be:
No Judgment / I don't know
Prohibitively expensive
Moderately expensive
Reasonable
Relatively cheap
Extremely cheap

Please list at least one relevant assumption that you made about reliance on human judgments.

16. Select all the components that would likely be contained in a Continuous Monitoring system for this type of risk (check all that apply). Leave this question blank if you believe none of the below are required or you don't have an opinion.
Analytical Functions (e.g., Regression Models, Expert Systems, Neural Nets, etc.)
Dashboard Reporting
Data Warehouse
Digital Agents (e.g., software that autonomously performs services or collects data)
Workflows (i.e., orchestrated and repeatable pattern of business activity supported by a systematic process)
Other (please specify)

RIM
by (Burr, Rothaermel et al. 2014)

In 1999, RIM introduced the BlackBerry 850 pager, which could receive push email from a Microsoft Exchange Server. In April 2000, the first BlackBerry smartphone, BlackBerry 957, was released. It included e-mail, paging and organizer features, as well as a 32-bit Intel 386 processor, 5MB flash memory, a QWERTY keyboard and an embedded wireless modem.

RIM experienced explosive growth in the early 2000s. Revenues were $85 million in 2000, which by 2007 increased to $3.04 billion and still showed signs of strong growth. During this period, gross margins had risen from 43% to 54.6%. In addition, RIM had

cultivated a cult following among customers. The term “CrackBerry” was coined to characterize Blackberry’s addictive nature. In 2007, RIM had a subscriber base of eight million.

However, Apple’s January 2007 introduction of the iPhone, which was dubbed the “Blackberry Killer”, marked the start of RIM’s decline. Competition increased again on October 22, 2008 when the first commercially available smartphone running Android was released. In 2009, RIM’s BlackBerry smartphone held a 20% share of the global market. However, by 2013, RIM’s global market share dropped to 1.9% while smartphones using Android and Apple respectively held 78.6% and 20% of the global smartphone market. In the third quarter of 2013, Windows Phones surpassed Blackberry as the third leading operating system for smartphones.

After 2007, analysts, investors and the media became increasingly concerned about RIM’s ability to compete. At the time, RIM’s hardware and operating system were criticized for being outdated and unappealing compared to their competition. Moreover, the Blackberry’s browsing capabilities were generally considered to be woefully inadequate compared to its competitors.

In September 2010, RIM announced the long rumored BlackBerry PlayBook tablet, officially released in April 2011. The PlayBook was criticized for being rushed to market in an incomplete state and sold poorly. Slow sales led to inventory pileups, which ultimately resulted in price cuts and a $485 million inventory write down.

In March 2011, RIM indicated that they planned to "launch some powerful new BlackBerrys." On January 2013, after much criticism and numerous delays, RIM officially launched two new smartphones, the BlackBerry Z10 and Q10, which thus far have sold poorly. In 2011, RIM felt that they owned the keyboard phone market and could afford to wait. However, the early promotion of these supposedly game changing devices may have hurt sales of BlackBerry’s existing products, which were already steadily losing market share.

In September 2011, which coincided with the launch of iPhone 4S, the RIM’s Internet Service suffered a massive outage, impacting millions of customers for several days. On August 12, 2013, Blackberry announced that it was open to being purchased, which is one of the reasons that it has been placed on the list of "10 Brands That Will Disappear in 2015."

For the above type of damage to brand risk scenario, please answer the following questions:

17. Can the data required to understand the current degree of this type of risk be obtained from current digital sources (e.g., databases or online sources, etc.)? (Ignore costs of access).

No Judgment / I don't know
None or very little of the data needed is in a digital form
Some of the relevant data is available digitally
About half of the relevant data is available digitally
Most of the relevant data is available digitally
All the relevant data is available digitally

18. Can a real time predictive model be constructed with a reasonable effort and investment within a one-year time horizon by an appropriate development group?

No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

Please list at least one assumption that you made about the use of data sources in a predictive model including any specific data related challenges related to integrating the data into the model.

19. Would reliance on human judgments (i.e., either internal expertise or professional consultants) be able to adequately detect changes in the degree of this risk?

No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

20. Relative to conventional human judgment, a real-time predictive model would be

No Judgment / I don't know
Far inferior in terms of accuracy, consistency and/or timeliness of predictions
Moderately inferior in terms of accuracy, consistency and/or timeliness of predictions
About the same
Moderately superior in terms of accuracy, consistency and/or timeliness of predictions
Far superior in terms of accuracy, consistency and/or timeliness of predictions

Please list at least one relevant assumption that you made in regards to this question

21. The cost of building a real-time predictive model for this risk would be:
No Judgment / I don't know
Extremely cheap
Relatively cheap
Reasonable
Moderately expensive
Prohibitively expensive

Please list at least one relevant assumption that you made about the cost of building this real-time predictive model.

22. The costs of relying on human judgments (i.e., either internal expertise or professional consultants) for this risk would be:
No Judgment / I don't know
Prohibitively expensive
Moderately expensive
Reasonable
Relatively cheap
Extremely cheap

Please list at least one relevant assumption that you made about reliance on human judgments.

23. Select all the components that would likely be contained in a Continuous Monitoring system for this type of risk (check all that apply). Leave this question blank if you believe none of the below are required or you don't have an opinion.
Analytical Functions (e.g., Regression Models, Expert Systems, Neural Nets, etc.)
Dashboard Reporting
Data Warehouse
Digital Agents (e.g., software that autonomously performs services or collects data)
Workflows (i.e., orchestrated and repeatable pattern of business activity supported by a systematic process)
Other (please specify)

APPENDIX C

ROUND 3 DELPHI AND POST-SURVEY QUESTIONS

This survey was implemented on Survey Monkey:

Directions for Round 3

Round 3, which is the final round, will focus on confirming or refuting the most popular assumptions made in Round 2, and give you a chance to revise your answers in light of these assumptions. The same Harvard Business School Cases will be used as a basis for Round 3. However, all the questions that didn't collect assumptions have been dropped. This round concludes with a few questions to assess the perceived quality of this research study.

If you have questions about this round or would like to interact more with your fellow research participants, please go to my WebBoard: http://baksaphd.activeboard.com/. Alternatively, you can email your questions directly to me at rbb25@njit.edu
You will be sent a concise summary of this Round's results within 60 days of the completion of this round. I will also notify you when my thesis has been completed. In case you would like to receive a copy.

1. Please Enter Your Full Name (i.e., First and Last)

2. Please enter your preferred email address?

Summary of Round 2 Results

Round 2 presented three Enterprise Risks: 1) Sony that dealt with cyber security; 2) Bear Stearns that dealt with operational risk; 3) RIM that dealt with Strategic Risk. The 188 respondents that completed Round 1 were sent the Round 2 survey. Round 2 had 81 respondents that completed the entire survey. The between round dropout rate was 57%.

Roughly half of the participants stated that each component (e.g., analytically components, dashboard reporting, data warehouses, and digital agents) were required on all three cases. No new architecture components where identified.

The Likert questions were constructed such that a higher Likert score indicated a more advantageous scenario for Continuous Monitoring. In aggregate, the results of Round 2 mirrored Round 1. Respondents in Round 2 ranked Sony as the most advantageous Continuous Monitoring case with a mean Likert score of 3.24 out of 5, which was followed by Bearn Stearns with a mean Likert score of 3.06 out of 5, while once again RIM was viewed the least advantageous case with a mean Likert score of 2.95 out of 5. Interestingly, there was an inverse relationship between a case's mean advantageous

score and its standard deviation. Blackberry had the highest aggregate standard deviation (1.15), followed by Bear Stearns (1.11), and then Sony (1.02). The high standard deviations represent disagreement between the respondents about the viability of Continuous Monitoring. The disagreement could result from the vastly different assumptions respondents made about the cases. Round 3 will explore the veracity of these assumptions.

Sony PlayStation: Security Breach
by (Seijts and Bigus 2012) HBS: W12309

Launched by Sony in 2010, Qriocity provided a cloud-based digital video and music service to consumers. Operated as a subscription service, Qriocity users set up an online account and paid a fee to access content. For Sony, Qriocity represented an opportunity to better integrate the company's consumer electronics with online music, movies and games. In 2011, Sony had over 350 million Internet-connected devices in use around the world, providing the company with a significant market of potential Qriocity customers.

Sometime between Sunday, April 17 and Tuesday, April 19, 2011, Sony's PlayStation and Qriocity user account information had been compromised as the result of an illegal intrusion into the company network. In response to this security threat, on Wednesday, April 20, 2011, Sony suspended all PlayStation and Qriocity networks services for 24 days, while Sony retained an external security firm to conduct a complete investigation of the incident. On May 4, Sony confirmed that personal information including names, birthdates, physical and e-mail addresses, network IDs and passwords, and possibly credit card information was stolen from its 77 million customers, which makes it one of the largest data security breaches in history. On May 23, Sony stated that this outage cost $171 million.

Sony had several security incidences before the attack. First, a month before the attack, the PlayStation.com website was a hacked by a group called Anonymous, apparently in response to Sony taking legal action against two modders, who are hackers that modify their consoles to give them additional functionality. Second, PlayStation 3 modders were claiming that PSN Web servers were running outdated versions of Apache and Linux, which had well known vulnerabilities. Finally, two weeks before the intrusion, Sony's networks were probed by a program that checks for known security vulnerabilities. Some speculate that if Sony had used an intrusion detection system prior to the attack, they may have noticed these vulnerabilities, which may have prompted them to heighten their defenses to guard against an attack.

Sony submitted written answers to questions posed by the United States House Subcommittee about this cyber-attack. Sony stated that they were the victim of a very carefully planned, professional, highly sophisticated criminal cyber-attack. The forensic teams were able to confirm the scope of the personal data they believed had been taken, and could not rule out that credit card information was also taken. They were taking a number of steps to prevent future breaches

For this type of cyber-attack risk scenario, please answer the following questions:

3. Below are the ten most frequently mentioned assumptions for the Sony case. Please state your opinion on their validity

	I Don't know / No Judgment	Always True	Generally True	Generally False	Always False
3.1) Standard data access patterns and exceptions to them can be readily defined and identified					
3.2) There exists publicly available data on past security breaches from other companies as well as known software and hardware security vulnerabilities					
3.3) All key infrastructure components are running operating systems and software that can be scanned using industry standard vulnerability detection software. This information can be easily accessed, aggregated and monitored.					
3.4) Cyber-attacks can happen very quickly. In milliseconds, large volumes of highly sensitive data can be stolen. As such, humans aren't well equipped to stop an in-flight cyber attack					
3.5) The number of possible security threats a large corporation such as Sony faces is nearly infinite and new threats appear all the time. As such, it would be very difficult for even a large team of security experts to manually review and process all the requisite information and data.					
3.6) Human and automated systems each have their own complementary strengths. An automated system is superior at real-time response or for implementing action as soon as a risk is detected. However, human judgment is superior at foreseeing possible threats/risks and initiating a course of action to mitigate these risks before they materialize.					
3.7) The large cost of building this security model could be spread across a large group of constituents, which would make the cost "reasonable" for each individual member.					
3.8) Sony's security needs can be adequately met by 3rd party package (e.g., Fireeye) with minimal customizations.					
3.9) The "cost" of relying on human judgment includes not just the cost to hire the personnel, but also the costs stem from a security breach					
3.10) Very experienced security experts have very high salaries					

Use the below text box to either clarify the above assumptions or list entirely new assumption(s) about this case. If you are commenting on an above assumption, please include its reference (e.g., 3.1, 3.2 …) in your response. Leave the below text box blank if the above accurately summaries your key assumptions

QUESTIONS 4 TO 8 BELOW REFER TO THE SONY CASE:
In light of the above assumptions that you feel are valid, please re-answer the below questions about this case

4. Can a real time predictive model be constructed with a reasonable effort and investment within a one-year time horizon by an appropriate development group?
No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

5. Relative to conventional human judgment, a real-time predictive model would be
No Judgment / I don't know
Far inferior in terms of accuracy, consistency and/or timeliness of predictions
Moderately inferior in terms of accuracy, consistency and/or timeliness of predictions
About the same
Moderately superior in terms of accuracy, consistency and/or timeliness of predictions
Far superior in terms of accuracy, consistency and/or timeliness of predictions

6. The cost of building a real-time predictive model for this risk would be:
No Judgment / I don't know
Extremely cheap
Relatively cheap
Reasonable
Moderately expensive
Prohibitively expensive

7. The costs of relying on human judgments (i.e., either internal expertise or professional consultants) for this risk would be:
No Judgment / I don't know
Prohibitively expensive
Moderately expensive
Reasonable
Relatively cheap
Extremely cheap

8. For this case, "Digital Agents" was the most frequently selected component in Round. Please briefly describe how it could be used in this Continuous Monitoring System

Bear Stearns
by (Rose, Bergstresser et al. 2009)

Founded in 1923, Bear Stearns & Co. (Bear) was the fifth largest U.S. investment bank in early 2008. However, it burned through nearly all of its $18 billion in cash reserves during the week of March 10, 2008. Bear's economic engine was its fixed income

business. In 2006, Bear's fixed income business contributed $3.62 billion in revenues, compared to $1.33 billion from investment banking and $1.38 billion from equities. Mortgages and mortgage-backed securities comprised most of the fixed income business, representing about 31% of the securities it owned. Bear was among the largest players in the mortgage market, and was the leading underwriter of U.S. mortgage backed securities from 2004 to 2007.

New financial market stresses, largely rooted in the U.S. housing market, emerged in 2007 and intensified in early 2008. Because home mortgages and home equity loans were frequently packaged and sold in securities that were in turn sold to a wide variety of investors, the rapid deterioration of housing prices was widely felt and created a heightened sense of anxiety across the financial markets. U.S. housing prices had appreciated rapidly between 1998 and 2006. This occurred alongside easier access to mortgage finance, especially among less credit-worthy borrowers. The origination of subprime mortgage loans grew from $190 billion in 2001 to $625 billion in 2005.

Even during auspicious periods, mortgage backed securities were often illiquid. As default rates rose and macroeconomic conditions deteriorated, the absence of a liquid trading market forced investors to seek bids from the commercial and investment banks that initially created and sold them. Wary of repurchasing too much of these securities, banks began to reduce the price they would pay and quantity they would buy for these securities. This only increased the downward pressure on bond prices, creating a "vicious circle" among the holders of mortgage backed securities: in addition to the uncertainty in fundamental value created by rising default rates, the reduction in prices by the bond dealers created even greater urgency on the part of investors to sell these securities, which forced the dealers to mark prices down even further. This vicious circle caused dealers, such as Bear, to accumulate larger and larger inventories of these securities, which were valued at perpetually lower prices.

Two large hedge funds managed by Bear Stearns had invested heavily in illiquid Collateralized Debt Obligations tied to mortgage backed securities. These funds had magnified their exposure to mortgage markets through the use of leverage; the fund managers were able to purchase as much as $60 worth of Collateralized Debt Obligations for each dollar invested. When these funds began selling assets to meet investor demands, it quickly led to the implosion of Bear. Bear survived to the close of business on Friday, March 14 only because of that morning's groundbreaking announcement: the Federal Reserve Bank of New York (N.Y. Fed), using JP Morgan Chase & Co. (JPMC) as a conduit, would provide Bear with secured financing for a period of up to 28 days. Despite this unprecedented provision of liquidity support, it was insufficient to reverse the decline in Bear's condition. On March 16, Bear's board accepted JPMC's offer to purchase Bear for $2 per share, which was subsequently increased to $10 a share.

For this type of liquidity risk scenario, please answer the following questions:

Below are the ten most frequently mentioned assumptions for the Bear Stearns case. Please state your opinion on their validity

	I Don't know / No Judgment	Always True	Generally True	Generally False	Always False
9.1) Time-series models of held inventory could provide a directional indication on where the market is heading.					
9.2) In general, modeling would have a difficult time predicting "black swan" events like this one because by definition there is very little (if any) historic data on this risk scenario					
9.3) While there is data that can indicate the absence of liquidity, by the time it is observed, it is likely to be too late to act on it.					
9.4) Experienced traders could predict this black swan event by generalizing from similar events that occurred in other markets.					
9.5) Markets are largely efficient and unpredictable. Even if the absence of liquidity could have been detected by a model, by the time it's detected it would likely be too late to do anything about it.					
9.6) If a sufficient number of data points could be aggregated from all market participants, adequate models could be constructed.					
9.7) In these high stake situations, a predictive model would be more impartial than human judgment, which could become clouded by greed and self interest					
9.8) Illiquid products are difficult to value, and hence, modeling them would be very difficult and costly.					
9.9) Ultimately, like all securities, the price of a MBS product depends on what the market will pay for it and that is not predictable in the short term					
9.10) These products are only understood by a handful of highly compensated traders and market participants. Consequently the costs to build these models would be very high.					

Use the below text box to either clarify the above assumptions or list entirely new assumption(s) about this case. If you are commenting on an above assumption, please include its reference (e.g., 9.1, 9.2 …) in your response. Leave the below text box blank if the above accurately summaries your key assumptions

QUESTIONS 10 TO 14 BELOW REFER TO THE SONY CASE:
In light of the above assumptions that you feel are valid, please re-answer the below questions about this case

10. Can a real time predictive model be constructed with a reasonable effort and investment within a one-year time horizon by an appropriate development group?

No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

11. Relative to conventional human judgment, a real-time predictive model would be
No Judgment / I don't know
Far inferior in terms of accuracy, consistency and/or timeliness of predictions
Moderately inferior in terms of accuracy, consistency and/or timeliness of predictions
About the same
Moderately superior in terms of accuracy, consistency and/or timeliness of predictions
Far superior in terms of accuracy, consistency and/or timeliness of predictions

12. The cost of building a real-time predictive model for this risk would be:
No Judgment / I don't know
Extremely cheap
Relatively cheap
Reasonable
Moderately expensive
Prohibitively expensive

13. The costs of relying on human judgments (i.e., either internal expertise or professional consultants) for this risk would be:
No Judgment / I don't know
Prohibitively expensive
Moderately expensive
Reasonable
Relatively cheap
Extremely cheap

14. For this case, "Data Warehouse" was the most frequently selected component in Round. Please briefly describe how it could be used in this Continuous Monitoring System

RIM
by (Burr, Rothaermel et al. 2014)

In 1999, RIM introduced the BlackBerry 850 pager, which could receive push email from a Microsoft Exchange Server. In April 2000, the first BlackBerry smartphone, BlackBerry 957, was released. It included e-mail, paging and organizer features, as well as a 32-bit Intel 386 processor, 5MB flash memory, a QWERTY keyboard and an embedded wireless modem.

RIM experienced explosive growth in the early 2000s. Revenues were $85 million in 2000, which by 2007 increased to $3.04 billion and still showed signs of strong growth. During this period, gross margins had risen from 43% to 54.6%. In addition, RIM had cultivated a cult following among customers. The term "CrackBerry" was coined to characterize Blackberry's addictive nature. In 2007, RIM had a subscriber base of eight million.

However, Apple's January 2007 introduction of the iPhone, which was dubbed the "Blackberry Killer", marked the start of RIM's decline. Competition increased again on October 22, 2008 when the first commercially available smartphone running Android was released. In 2009, RIM's BlackBerry smartphone held a 20% share of the global market. However, by 2013, RIM's global market share dropped to 1.9% while smartphones using Android and Apple respectively held 78.6% and 20% of the global smartphone market. In the third quarter of 2013, Windows Phones surpassed Blackberry as the third leading operating system for smartphones.

After 2007, analysts, investors and the media became increasingly concerned about RIM's ability to compete. At the time, RIM's hardware and operating system were criticized for being outdated and unappealing compared to their competition. Moreover, the Blackberry's browsing capabilities were generally considered to be woefully inadequate compared to its competitors.

In September 2010, RIM announced the long rumored BlackBerry PlayBook tablet, officially released in April 2011. The PlayBook was criticized for being rushed to market in an incomplete state and sold poorly. Slow sales led to inventory pileups, which ultimately resulted in price cuts and a $485 million inventory write down.

In March 2011, RIM indicated that they planned to "launch some powerful new BlackBerrys." On January 2013, after much criticism and numerous delays, RIM officially launched two new smartphones, the BlackBerry Z10 and Q10, which thus far have sold poorly. In 2011, RIM felt that they owned the keyboard phone market and could afford to wait. However, the early promotion of these supposedly game changing devices may have hurt sales of BlackBerry's existing products, which were already steadily losing market share.

In September 2011, which coincided with the launch of iPhone 4S, the RIM's Internet Service suffered a massive outage, impacting millions of customers for several days. On August 12, 2013, Blackberry announced that it was open to being purchased, which is one of the reasons that it has been placed on the list of "10 Brands That Will Disappear in 2015."

For the above type of damage to brand risk scenario, please answer the following questions:

15. Below are the ten most frequently mentioned assumptions for the RIM case. Please state your opinion on their validity

	I Don't know / No Judgment	Always True	Generally True	Generally False	Always False
15.1) Innovation is still strictly a human endeavor, modeling it would be a limited value					
15.2) Basic market research, customer polls, and declining sales trend could have provided a strong leading indicator to the downfall RIM's dominance.					
15.3) Detecting RIM's declining sales could be done adequately well by either a human or a predictive algorithm. However, only a human could formulate and implement a strategic vision to reverse this trend					
15.4) A predictive model could pull information from the web by scanning Facebook postings, twitter feeds, etc. to predict RIM's looming decline					
15.5) This predictive model doesn't need to be real time. It could safely be run monthly quarterly, or even yearly					
15.6) Experts have a very tough time predicting which products will be "hot" and which products will fall out of favor					
15.7) Highly creative people are expensive					
15.8) In RIM's situation, human judgment was blinded by over confidence					
15.9) The market forces that led to RIM's decline were so unique that building a predictive model for them would be prohibitively expensive and, probably not very reusable					
15.10) Apple and Android's ultimate success in the market place couldn't be predicted by any means					

Use the below text box to either clarify the above assumptions or list entirely new assumption(s) about this case. If you are commenting on an above assumption, please include its reference (e.g., 15.1, 15.2 …) in your response. Leave the below text box blank if the above accurately summaries your key assumptions

QUESTIONS 16 TO 20 BELOW REFER TO THE RIM CASE:
In light of the above assumptions that you feel are valid, please re-answer the below questions about this case

16. Can a real time predictive model be constructed with a reasonable effort and investment within a one-year time horizon by an appropriate development group?

No Judgment / I don't know
Definitely Infeasible
Possibly Infeasible
Feasible
Possibly Feasible
Definitely Feasible

17. Relative to conventional human judgment, a real-time predictive model would be
No Judgment / I don't know
Far inferior in terms of accuracy, consistency and/or timeliness of predictions
Moderately inferior in terms of accuracy, consistency and/or timeliness of predictions
About the same
Moderately superior in terms of accuracy, consistency and/or timeliness of predictions
Far superior in terms of accuracy, consistency and/or timeliness of predictions

18. The cost of building a real-time predictive model for this risk would be:
No Judgment / I don't know
Extremely cheap
Relatively cheap
Reasonable
Moderately expensive
Prohibitively expensive

19. The costs of relying on human judgments (i.e., either internal expertise or professional consultants) for this risk would be:
No Judgment / I don't know
Prohibitively expensive
Moderately expensive
Reasonable
Relatively cheap
Extremely cheap

20. For this case, "Analytical Functions" was the most frequently selected component in Round 2. Please briefly describe how they could be used in this Continuous Monitoring System.

Post Survey Questions

21. Did you obtain useful information from this study?
None
Not much
A few pieces of useful information
Some useful information
Lots of useful information

22. What is the potential importance of this study's results?
Irrelevant
Not very important
Somewhat important
Important
Very Important

23. To what extent do you believe that Continuous Monitoring has the potential to provide material business value to today's companies?

Very Likely
Likely
Neither Likely or Unlikely
Unlikely
Very Unlikely

24. What was the overall quality of this study?

Very Low
Low
Medium
High
Very high

REFERENCES

(2006). "International Convergence of Capital Measurement and Capital Standards." from http://www.bis.org/publ/bcbs128.pdf.

(2009). "Improving the Analytical Process with XBRL." Retrieved 8/31/09, 2009, from http://www.xbrl.us/Learn/Documents/XBRLforAnalysts.pdf.

(2009). "Remarks by the President on 21st Century Financial Regulatory Reform." from http://www.whitehouse.gov/the_press_office/Remarks-of-the-President-on-Regulatory-Reform/.

(2010). "Continuous Monitoring and Continuous Auditing From idea to implementation." from http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_continuous_monitoring_and_continuous_auditing_whitepaper_102910.pdf.

(2010). "What is Driving Continuous Auditing and Monitoring Today?", from https://www.in.kpmg.com/SecureData/aci/Files/CA_Cam_WhitePaper_Final_WEB.pdf.

(2011). "Deloitte Continues as an Engine of Employment Creation and Announces Record Revenues of US $28.8 Billion." from http://www.deloitte.com/view/en_GX/global/press/global-press-releases-en/96616a3cfdc82310VgnVCM1000001a56f00aRCRD.htm.

(2011). "Ernst & Young Reports Fiscal Year 2011 Global Revenues of US$22.9 Billion." from http://www.ey.com/GL/en/Newsroom/News-releases/Ernst-and-Young-reports-2011-global-revenues-of-US-dollar-22-9-billion.

(2011). "Financial Regulatory Reform." The New York Times, from http://topics.nytimes.com/topics/reference/timestopics/subjects/c/credit_crisis/financial_regulatory_reform/index.html.

Ackoff, R. L. (1967). "Management Misinformation Systems." Management Science **14**(4): B-147-B-156.

ACL. (2006). "Continuous Auditing." Retrieved 8/29/2009, from http://www.aclchina.com/solution/Continuous%20Auditing.pdf.

ACL. (2006). "New Demands, New Priorities The Evolving Role of Internal Audit." Retrieved 8/22/09, from http://www.acl.com/PDFs/caesurvey_results06.pdf.

Aguilar, M. (2008, December 23, 2008). "SEC Mandates XBRL Filings by July 2009." Compliance Week, from http://www.complianceweek.com/article/5197/sec-mandates-xbrl-filings-by-july-2009.

Alexander, J. (2002). "History of Accounting." from http://documents.clubexpress.com/documents.ashx?key=7ZPfhrgSH4ej5qOo06gTZ1j%2FWfzYw%2BhpXBNOQ%2BbRiWgYV1UQpbPezRxbi%2FPDVo7X.

Alles, M., G. Brennan, et al. (2006). "Continuous Monitoring of Business Process Controls: A Pilot Implementation of a Continuous Auditing System at Siemens." International Journal of Accounting Information Systems **7**(2): 137-161.

Alles, M. and A. Kogan (2003). "Black box Logging and Tertiary Monitoring of Continuous Assurance Systems." Information Systems Audit and Control Association **1**: 4.

Alles, M., A. Kogan, et al. (2004). "Restoring Auditor Credibility: Tertiary Monitoring and Logging of Continuous Assurance Systems." International Journal of Accounting Information Systems **5**(2): 183-202.

Alles, M., A. Kogan, et al. (2013). "Collaborative Design Research: Lessons from Continuous Auditing." International Journal of Accounting Information Systems **14**(2): 104-112.

Alles, M., A. Kogan, et al. (2008). Audit Automation as the Foundation of Continuous Auditing. 16th World Continuous Auditing & Reporting Symposium. Rutgers Business School - Newark, New Jersey.

Alomari, R. (2004). "A Fragile Watermarking Algorithm for Content Authentication." International Journal of Computing & Information Sciences **2**(1).

Alviniussen, A. and H. Jankensgård (2009). "Enterprise Risk Budgeting: Bringing Risk Management Into the Financial Planning Process." Journal of Applied Finance **19**(1/2): 178-192.

ANSI/IEEE (2000). Recommended Practice for Architectural Description of Software-Intensive Systems**:** 23.

Approva. (2009). "Continuous Controls Monitoring Accounts Payable Insight." Retrieved 8/28/2009, 2009, from http://www.approva.net/assets/resources/DS_AccountsPayable.pdf.

Bach, J. (1999). "Test Automation Snake Oil." Retrieved V2.1, from http://www.satisfice.com/articles/test_automation_snake_oil.pdf.

Bailey James, S. W. P. (1983). "Development of a Tool for Measuring and Analyzing Computer User Satisfaction." Management Science **29**(4): 17.

Baker, N. and T. McCollum (2005). "Fraud and Artificial Intelligence." Internal Auditor **62**(1): 29-32.

Bakhtiari, S., R. Safavia-naini, J. Pieprzyk. (1995). "Cryptographic Hash Functions: A Survey." from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.56.8428&rep=rep1&type=pdf.

Baksa, R., M. Turoff, et al. (2010). Continuous Auditing as a Foundation for Real Time Decision Support: Implementation Challenges and Successes. New York, NY, Springer. **13:** 237-252.

Bañuls, V. A. and M. Turoff (2011). "Scenario Construction via Delphi and Cross-Impact Analysis." Technological Forecasting and Social Change **78**(9): 1579-1602.

Bañuls, V. A., M. Turoff, et al. (2013). "Collaborative Scenario Modeling in Emergency Management through Cross-Impact." Technological Forecasting and Social Change **80**(9): 1756-1774.

Barton, T. L., W. G. Shenkir, et al. (2009). "ERM: The Evolution of a Balancing Act." Financial Executive **25**(10): 10-14.

Basel. (2001). "Operational Risk." from https://www.bis.org/publ/bcbsca07.pdf.

Bazerman, M. H., G. Loewenstein, et al. (2002). "Why Good Accountants Do Bad Audits." Harvard Business Review **80**(11): 96-103.

Beasley, M., B. Branson, et al. (2009). "ERM: Opportunities for Improvement." Journal of Accountancy **208**(3): 28-32.

Beasley, M., R. Clune, et al. (2005). "ERM a Status Report." Internal Auditor **62**(1): 67-72.

Berinato, S. (2004, December 16, 2004). "Risk's Rewards." CIO, from http://www.cio.com.au/article/print/181713/risk_rewards/.

Berner, R. (2013). "2013 Annual Report." from http://www.treasury.gov/initiatives/ofr/about/Documents/OFR_AnnualReport2013_FINAL_12-17-2013_Accessible.pdf.

Berner, S., R. Weber, et al. (2005). Observations and Lessons Learned from Automated Testing. Proceedings of the 27th international conference on Software engineering. St. Louis, MO, USA, ACM.

Bernstein, P. (1996). Against the Gods: The Remarkable Story of Risk. Hoboken, NJ, John Wiley & Sons, Inc.

Blenko, M. and M. Mankins. (2012). "Measuring Decision Effectiveness." Insights, from http://www.bain.com/publications/articles/measuring-decision-effectiveness.aspx.

Bloch, M., B. Sven, et al. (2012). "Delivering Large-scale IT Projects on Time, on Budget, and on Value." from http://www.mckinsey.com/insights/business_technology/delivering_large-scale_it_projects_on_time_on_budget_and_on_value.

Botosan, C. (1997). "Disclosure Level and the Cost of Equity Capital." Accounting Review **72**(3): 323.

Bovee, M., A. Kogan, et al. (2005). "Financial Reporting and Auditing Agent with Net Knowledge (FRAANK) and extensible Business Reporting Language (XBRL)." Journal of Information Systems **19**(1): 19-41.

Bowles, M. and J. Lu (2014). "Removing the Blinders: A Literature Review on the Potential of Nanoscale Technologies for the Management of Supply Chains." Technological Forecasting and Social Change **82**(0): 190-198.

Brace, J., C. Rozwell, et al. (2006) "Understanding the Costs of Compliance." 19.

Brennan, G. (2008). "Continuous Auditing Comes of Age." Information Systems Audit and Control Association.

Brooks, D. (2013, February 18, 2013). "What Data Can't Do." The New York Times, from http://www.nytimes.com/2013/02/19/opinion/brooks-what-data-cant-do.html?_r=0.

Burr, J., F. Rothaermel, et al. (2014). "Make or Break at RIM (in 2013): Launching BlackBerry 10." Harvard Business School.

Calderon, T. and J. Cheh (2002). "A Roadmap for Future Neural Networks Research in Auditing and Risk Assessment." International Journal of Accounting Information Systems **3**(4): 203-236.

Caldwell, F., T. Eid, et al. (2009). Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms, Gartner**:** 21.

Caldwell, F. and P. Proctor. (2009). "Continuous Controls Monitoring for Transactions: The Next Frontier for GRC Automation."

Caldwell, F. and P. Proctor. (2010, March 23, 2010). "Magic Quadreant for Continuous Controls Monitoring."

Caldwell, F., J. Wheatman, et al. (2009). "Predicts 2010: Comprehensive Governance, Risk and Compliance Remains Elusive."

CAS. (2003). "Overview of Enterprise Risk Management." from http://www.casact.org/area/erm/overview.pdf.

Cash Jr, J., A. Bailey Jr, et al. (1977). "A Survey of Techniques for Auditing EDP-Based Accounting Information Systems." Accounting Review **52**(4): 813-832.

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

Chan, S. (2001). "The Use of Graphs as Decision Aids in Relation to Information Overload and Managerial Decision Quality." Journal of Information Science **27**(6): 417-426.

Chan, S. and S. Wright (2007). "Feasibility of More Frequent Reporting: A Field Study Informed Survey of In-Company Accounting and IT Professionals." Journal of Information Systems **21**(2): 101-115.

Chewning, E. and A. Harrell (1990). "The Effect of Information Load on Decision Makers' Cue Utilization Levels and Decision Quality in a Financial Distress Decision Task." Accounting, Organizations and Society **15**(6): 527-542.

CICA/AICPA. (1999). "Continuous Auditing, Research Report." from http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper_current-state-continuous-auditing-monitoring.pdf.

Clancy, H. (2014, October 10 2014). "How GE generates $1 Billion from Data." Fortune, from http://fortune.com/2014/10/10/ge-data-robotics-sensors/.

Coakley, J. (1995). "Using Pattern Analysis Methods to Supplement Attention Directing Analytical Procedures." Expert Systems with Applications **9**(4): 513-528.

Coderre, D. (2005). Global Technology Audit Guide Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment**:** 44.

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

Coderre, D. (2009). Internal Audit: Efficiency through Automation. Hoboken, New Jersey, John Wiley & Sons.

Coletti, A., K. Sedatole, et al. (2005). "The Effect of Control Systems on Trust and Cooperation in Collaborative Environments." Accounting Review **80**(2): 477-500.

Cook, G. (1993). "An Empirical Investigation of Information Search Strategies with Implications for Decision Support System Design." Decision Sciences **24**: 683-699.

COSO. (2004, September 2004). "Enterprise Risk Management - Integrated Framework." from http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.

Cumming, C. and B. Hirtle (2001). "The Challenges of Risk Management in Diversified Financial Companies." FRBNY Economic Policy Review **March**.

Curtis, M. and E. Payne (2008). "An Examination of Contextual Factors and Individual Characteristics Affecting Technology Implementation Decisions in Auditing." International Journal of Accounting Information Systems **9**(2): 104-121.

D2K. (2005). "D2K Developer White Paper." from http://www.d2k.com/d2k/pdf/D2K_Developer_White_Paper.pdf.

D'Arcy, S. (2001). "Enterprise Risk Management " Journal of Risk Management of Korea **12**(1).

Davenport, T. and L. Prusak (2000). Working Knowledge. Boston, Massachusetts, Harvard Business Review Press; 2nd edition (May 2000).

Davies, M. (2011). "PwC Reports FY2011 Global Revenues of US$29.2 Billion." from http://press.pwc.com/GLOBAL/News-releases/pwc-reports-fy2011-global-revenues-of-us29.2-billion/s/f2d3a043-5a2c-4293-b59a-0d3744baa9b0.

Davis, J., A. Massey, et al. (1997). "Supporting a Complex Audit Judgment Task: An Expert Network Approach." European Journal of Operational Research **103**(2): 350-372.

Debreceny, R. and G. Gray (2001). "The Production and Use of Semantically Rich Accounting Reports on the Internet: XML and XBRL." International Journal of Accounting Information Systems **2**(1): 47-74.

Debreceny, R., G. Gray, et al. (2005). "Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Functionality." Journal of Information Systems **19**(2): 7-27.

Denton, K. (2001). "Better Decisions." Industrial Management **43**(4): 21.

Deshmukh, A., S. Nassiripor, et al. (1998). Applications of Fuzzy Sets and The Theory of Evidence to Accounting II Assessment of Short-Term Liquidity Risk Using Fuzzy Sets:. Greenwich, CT, JAI Press Inc.

Deshmukh, A., J. Romine, et al. (1998). A Fuzzy Set Approach to Client Acceptance Decisions Applications of Fuzzy Sets and The Theory of Evidence to Accounting, II. Greenwich, CT, JAI Press Inc.

Devlin, H. (2015, February 4, 2015). "Rise of the Robots: How Long Do We Have Until They Take Our Jobs?" The Guardian, from http://www.theguardian.com/technology/2015/feb/04/rise-robots-artificial-intelligence-computing-jobs.

Dewhurst, M. and P. Willmott (2014). "Manager and Machine: The New Leadership Equation." McKinsey Quarterly.

Dhar, V. and R. Stein (1997). Intelligent Decision Support Methods. Upper Saddle River, NJ, Prentice-Hall, Inc.

Dionne, G. (2013). "Risk Management: History Definition and Critique." from https://www.cirrelt.ca/DocumentsTravail/CIRRELT-2013-17.pdf.

Dowling, C. and S. Leech (2007). "Audit Support Systems and Decision Aids: Current Practice and Opportunities for Future Research." International Journal of Accounting Information Systems **8**(2): 92-116.

Edmunds, A. and A. Morris (2000). "The Problem of Information Overload in Business Organizations: A Review of the Literature." International Journal of Information Management **20**(1): 17-28.

Eining, M., D. Jones, et al. (1997). "Reliance on Decision Aids: An Examination of Auditors' Assessment of Management Fraud." Auditing: A Journal of Practice and Theory **16**(2): 19.

Elliott, R. (2002). "Twenty-First Century Assurance." Auditing **21**(1): 139.

Etheridge, H., R. Sriram, et al. (2000). "A Comparison of Selected Artificial Neural Networks that Help Auditors Evaluate Client Financial Viability." Decision Sciences **31**(2): 531-550.

Etzioni, A. (2001). Humble Decision Making Harvard Business Review on Decision Making. Boston, Massachusetts, Harvard Business Press.

Fedorowicz, J. (2008). "Managing Risk Through Financial Processes: Embedding Governance, Risk and Compliance." The Economist: 23.

FEI. (2008). "FEI Survey: Average 2007 SOX Compliance Cost $1.7 Million." from http://fei.mediaroom.com/index.php?s=43&item=204.

Fischer, M. (1996). ""Real-izing" The Benefits of New Technologies as a Source of Audit Evidence: An Interpretive Field Study." Accounting, Organizations and Society **21**(2-3): 219-242.

Flynn, T. (2011). "KPMG International Annual Review 2010." from http://www.kpmg.com/Global/en/WhoWeAre/Performance/AnnualReviews/Documents/KPMG-International-Annual-Review-2010.pdf.

Ford, M. (2009). "The Lights in the Tunnel: Automation, Accelerating Technology and the Economy of the Future."

Gordon, T. and O. Helmer (1964). Report on a Long Range Forecasting Study. Rand Corporation. Santa Monica.

Gorr, W. (2009). "Forecast Accuracy Measures for Exception Reporting Using Receiver Operating Characteristic Curves." International Journal of Forecasting **25**(1): 48-61.

Greco, S., B. Matarazzo, et al. (1998). A New Rough Set Approach to Evaluation of Bankruptcy Risk Operational Tools in the Management of Financial Risks. New York, NY, Springer.

Grise, M. and B. Gallupe (1999). "Information Overload: Addressing the Productivity Paradox in Face-to-Face Electronic Meetings." Journal of Management Information Systems **16**(3): 157-185.

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

Hall, B. and B. Khan. (2003). "Adoption of New Technology." from http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1055&context=iber/econ.

Hammond, J., R. Keeney, et al. (2001). The Hidden Traps in Decision Making: Harvard Business Review on Decision Making. Boston, Massachusetts, Harvard Business Press.

Hammond, J., R. Keeney, et al. (2001). The Rational Method for Making Trade-offs: Harvard Business Review on Decision Making, Harvard Business Press**:** 224.

Hannon, N. (2005). Enterprise Business Reporting in the Post Sarbanes-Oxley Era: A Data-Centric Approach. 10th World Continuous Auditing and Reporting Symposium. Rutgers Business School - Newark, New Jersey, USA.

Harrison, R. (2005). "Embracing Compliance with Continuous Online Auditing." Sarbanes-Oxley Compliance Journal: 4.

Helms, G., J. Mancino, et al. (1999). "Information Technology Issues for the Attest, Audit, and Assurance Services Functions." CPA Journal **69**(5): 62.

Heng Yik, S., Y. Jifeng, et al. (2011). "Enterprise Risk Management in Financial Crisis." IUP Journal of Risk & Insurance **8**(3): 7-21.

Hian Chye, K. and T. Sen Suan (1999). "A Neural Network Approach to the Prediction of Going Concern Status." Accounting & Business Research **29**(3): 211-216.

Hiltz, R. and M. Turoff (1985). "Structuring Computer-Mediated Communication Systems to Avoid Information Overload." Commun. ACM **28**(7): 680-689.

Höne, K. and J. Eloff (2002). "Information Security Policy -- What Do International Information Security Standards Say?" Computers & Security **21**(5): 402-409.

Hoxmeier, J. and C. DiCesare (2000). System Response Time and User Satisfaction: An Experimental Study of Browser-Based Applications. Proceedings of the Association of Information Systems Americas Conference. Long Beach, California.

Hoyt, R. and A. Liebenbergerg. (2008). "The Value of Enterprise Risk Management." from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1440947.

Hsu, W. and S. Ong. (2004). "Fossilization: A Process for Establishing Truly Trustworthy Records." from http://domino.watson.ibm.com/library/cyberdig.nsf/papers/02DA1CEA05C6C61D85256F3A0069DCA0/$File/rj10331.pdf.

Hulstijn, J., R. Christiaanse, et al. (2011). Continuous Control Monitoring-Based Regulation: A Case in the Meat Processing Industry Advanced Information Systems Engineering Workshops. W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw and C. Szyperski. Berlin, Germany, Springer **83:** 238-248.

Hunton, J. (2002). Assessing The Impact of More Frequent External Financial Statement Reporting and Independent Auditor Assurance on Quality of Earnings and Stock Market Effects. The Fifth Continuous Auditing Symposium. Rutgers Business School.

Jablecki, J. (2009). "The Impact of Basel I Capital Requirements on Bank Behavior and the Efficacy of Monetary Policy." International Journal of Economic Sciences and Applied Research **2**(1): 16-35.

Jacoby, J., D. Speller, et al. (1974). "Brand Choice Behavior as a Function of Information Load: Replication and Extension." Journal of Consumer Research **1**(1): 33-42.

Kaufman, L. (2009). "Data Security in the World of Cloud Computing." Security & Privacy, IEEE **7**(4): 61-64.

Kent, R., A. H. Zahid, et al. (2011). Continuous Auditing for Health Care Decision Support Systems Intelligent Decision Technologies. R. J. Howlett and L. C. Jain. Berlin, Germany, Springer **10:** 731-741.

King, T. (2006). More Than a Numbers Game: A Brief History of Accounting, Wiley.

Knechel, R. (1988). "The Effectiveness of Statistical Analytical Review as a Substantive Auditing Procedure: A Simulation Analysis." Accounting Review **63**(1): 74.

Ko, R., S. Lee, et al. (2009). "Business Process Management (BPM) Standards: A Survey." A Survey. In: Business Process Management Journal **15**(5).

Koskivaara, E. (2000). "Artificial Neural Network Models for Predicting Patterns in Auditing Monthly Balances." J Oper Res Soc **51**(9): 1060-1069.

KPMG. (2011). "Insurance Regulation – On the Move." from http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/insurance-regulation-on-the-move/Documents/KPMG%20On%20the%20Move-Sept-2011.pdf.

Krass, P. (2002). "The Never-ending Audit." CFO **18**(10): 25.

Krell, E. (2009). "Monitoring Matter." Business Finance, from http://businessfinancemag.com/risk-management/monitoring-matters.

Kuenkaikaew, S. (2008). Experience of Leading Edge Organizations with CA/CM: Understanding the Challenges around People, Process and Technology. Sixteenth World Continuous Auditing & Reporting Symposium, Rutgers Business School, 180 University Avenue Lecture Hall – Room 123 – Ackerson Hall – 1st floor, Newark, NJ 07102.

Kuhn, R. and S. Sutton (2010). "Continuous Auditing in ERP System Environments: The Current State and Future Directions." Journal of Information Systems **24**(1): 91-112.

Kuhn, R. and S. Sutton (2006). "Learning from WorldCom: Implications for Fraud Detection through Continuous Assurance." Journal of Emerging Technologies in Accounting **3**(1): 61-80.

Lawrence, Q. (2005, January / February 2005). "ERM Embracing A Total Risk Model." Financial Executive, from http://www.jameslam.com/Articles/Financial%20Executive%20International%20Embracing%20a%20total%20risk%20model%20Feb%202005.pdf.

Lazanis, R. (2015, January 22, 2015). "How Technology Behind Bitcoin Could Transform Accounting As We Know It." TechVibes, from http://www.techvibes.com/blog/how-technology-behind-bitcoin-could-transform-accounting-as-we-know-it-2015-01-22.

Lin, J. and J. Hwang (2003). "A Fuzzy Neural Network for Assessing the Risk of Fradulent Financial Reporting." Managerial Auditing Journal **8**(18): 9.

Lindberg, D. and D. Seifert (2011). "Enterprise Risk Management (ERM) Can Assist Insurers in Complying with the Dodd-Frank Act." Journal of Insurance Regulation **30**: 319-337.

Linstone, H. and M. Turoff (1975). The Delphi Method: Techniques and Applications.

Linstone, H. and M. Turoff (2011). "Delphi: A Brief Look Backward and Forward." Technological Forecasting and Social Change **78**(9): 1712-1719.

Loch, K., H. Carr, et al. (1992). "Threats to Information Systems: Today's Reality, Yesterday's Understanding." MIS Quarterly **16**(2): 173-186.

Loeb, D. (2006, December 5, 2009). "Once Again, Machine Beats Human Champion at Chess " The New York Times, from http://www.nytimes.com/2006/12/05/crosswords/chess/05cnd-chess.html?_r=1.

Makomaski, J. (2008). "So What Exactly Is ERM?" Risk Management (00355593) **55**(4): 80-81.

Malone, T., K. Crowston, et al. (2003). Organizing Business Knowledge: the MIT Process Handbook. Boston, Massachusetts, The MIT Press.

Manyika, J., M. Chui, et al. (2011). "Big data: The Next Frontier for Innovation, Competition and Productivity." from http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation.

Marchand, D., W. Kettinger, et al. (2000). "Information Orientation: People, Technology and the Bottom Line." Sloan Management Review **41**(4): 69-80.

Markoff, J. (2011). Computer Wins on 'Jeopardy!': Trivial It's Not. The New York Times.

Markoff, J. (2012, November 23, 2012). "Scientists See Promise in Deep-Learning Programs." New York Times, from http://www.nytimes.com/2012/11/24/science/scientists-see-advances-in-deep-learning-a-part-of-artificial-intelligence.html?_r=0.

Markus, L. (1983). "Power, Politics, and MIS Implementation." Commun. ACM **26**(6): 430-444.

McKinsey. (2014). "Artificial Intelligence Meets the C-suite." McKinsey Quarterly, September 2014.

Means, G. and D. Warren. (2005). "Continuous Financial Controls Review Processes." Sarbanes-Oxley Compliance Journal, from http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=417.

Mehr, R. and B. Hedge (1963). Risk Management in the Business Enterprise. Homewood, Illinois, Irwin.

Mehra, M. (2006). "Sarbanes-Oxley Three Years On." from http://www.wcfcg.net/Sarbanes-Oxley%20Three%20Years%20On.pdf.

Meulbroek, L. (2002). "Integrated Risk Management for the Firm: A Senior Manager's Guide " Harvard Business School, from http://www.outsourcerm.com/files/integrated_rm_for_the_firm.pdf.

Moody's. (2012). "Basel III New Capital and Liquidity Standards - FAQs." from http://www.moodysanalytics.com/~/media/Insight/Regulatory/Basel-III/Thought-Leadership/2012/2012-19-01-MA-Basel-III-FAQs.ashx.

Morieux, Y. and P. Tollman (2014). Six Simple Rules: How to Manage Complexity without Getting Complicated. Boston, Massachuetts, Havard Business School Publishing.

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

Murthy, U. and M. Groomer (2004). "A Continuous Auditing Web Services Model for XML-based Accounting Systems." International Journal of Accounting Information Systems **5**(2): 139-163.

Negus, J. (2010, March 1, 2010). "10 Common ERM Challenges." Risk Management from http://www.rmmagazine.com/2010/03/01/10-common-erm-challenges/.

Nocco, B. (2006). "Enterprise Risk Management: Theory and Practice." Journal of Applied Corporate Finance **18**(4).

OCC. (1998). "Emerging Market Country Products and Trading Activities." from http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/emkt.pdf.

Olsen, K., K. Sochats, et al. (1998). "Full Text Searching and Information Overload." The International Information & Library Review **30**(2): 105-122.

ORX. (2012). "2012 ORX Report on Operational Risk Loss Data." from https://www.orx.org/Pages/orxdata.aspx.

Ovans, A. (2012, December 6, 2012). "Morning Advantage: Lessons from the Worst-Performing Companies in America." Harvard Business Review, from http://blogs.hbr.org/morning-advantage/2012/12/morning-advantage-lessons-from.html.

Paape, L. and R. Speklé (2012). "The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study." European Accounting Review **21**(3): 533-564.

Parenté, F., J. Anderson, et al. (1984). "An Examination of Factors Contributing to Delphi Accuracy." Journal of Forecasting **3**(2): 173-182.

Patten, K., J. Fjemestad, et al. (2009). How CIOs Use Flexibility to Manage Uncertainty in Dynamic Business Environments. 15th Americas Conference on Information Systems, San Francisco, California, USA.

Pavlou, K. (2011). "Database Forensics in the Service of Information Accountability." from http://www.cs.arizona.edu/~kpavlou/idar2011-pavlou.pdf.

Penler, P. (2006). Panel Discussion on Continuous Auditing. 12th World Continuous Auditing and Reporting Symposium. Rutgers Business School - Newark, New Jersey, USA.

Peterson, M. (2004). "Information: Hard and Soft." from http://www.disas.unisi.it/mat_did/gabbi/729/10.1.1.126.8246[1].pdf.

Power, D. (2007). "A Brief History of Decision Support Systems." from http://DSSResources.COM/history/dsshistory.html.

Power, M. (1999). The Audit Society: Rituals of Verification. New York, NY, Oxford University Press.

Proctor, P. and F. Caldwell (2010). Critical Capabilities for Continuous Controls Monitoring, Gartner.

Protess, B. (2011). "Dodd-Frank Inches Along." The New York Times, from http://dealbook.nytimes.com/2011/09/06/dodd-frank-inches-along/?scp=17&sq=Frank%20Dodd%20Act&st=cse.

Pyzdek, T. (2009). The Six Sigma Handbook. New York, NY, McGraw-Hill Professional.

Ramamoorti, S., A. Bailey, et al. (1999). "Risk Assessment in Internal Auditing: a Neural Network Approach." International Journal of Intelligent Systems in Accounting, Finance & Management **8**(3): 159-180.

Ramamoorti, S., M. Cangemi, et al. (2010). "The Benefits of Continuous Monitoring." from http://raw.rutgers.edu/docs/wcars/23wcars/Presentations/Mike%20Cangemi-The_Benefits_of_Continuous_Monitoring_edited_final_8-11[1].pdf.

Ramler, R. and K. Wolfmaier (2006). Economic Perspectives in Test Automation: Balancing Automated and Manual Testing with Opportunity Cost. Proceedings of the 2006 international workshop on Automation of software test. Shanghai, China, ACM.

Ratley, J. (2008). "2008 Report to the Nation on Occupational Fraud and Abuse." from http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/2008-rttn.pdf.

Razali, A. and I. Tahir (2011). "Review of the Literature on Enterprise Risk Management." Business Management Dynamics **1**(5): 08-16.

Redgrave, J., A. Prasad, et al. (2005). "The SEDONA Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production." The SEDONA Conference, from www.thesedonaconference.org.

Redman, T. (2014, September 17, 2014). "Algorithms Make Better Predictions - Except When They Don't." Harvard Business Review, from https://hbr.org/2014/09/algorithms-make-better-predictions-except-when-they-dont/.

Redman, T. and D. Hay. (2012, December 13, 2012). "Effective Regulation Requires Information Richness." Harvard Business Review, from http://blogs.hbr.org/cs/2012/12/effective_regulation_requires.html.

Reinhart, C. and K. Rogoff (2011). This Time Is Different: Eight Centuries of Financial Folly. Princeton University Press.

Rezaee, Z., Ahmand Shartbatoghlie, Rick Elam and Peter McMickle (2002). "Continuous Auditing: Building Automated Auditing Capability." Auditing: A Journal of Practice and Theory **Vol 21**(No. 1).

Rezaee, Z., R. Elam, et al. (2001). "Continuous Auditing: the Audit of the Future." Managerial Auditing Journal **16**(3): 150 - 158.

Riley, M., B. Elgin, et al. (2014, March 12, 2014). "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." Bloomberg Business Week, from http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

Roebuck, K. (2011). Continuous Integration: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors. Ruislip, Middlesex United Kingdon, Tebbo.

Roethlisberger, F. and W. Dickson (1939). Management and the Worker: An Account of a Research Program Conducted by the Western Electric Company, Hawthorne Works, Chicago. Boston, Massachusetts, Harvard University Press.

Rose, C., D. Bergstresser, et al. (2009). "The Tip of the Iceberg: JP Morgan Chase and Bear Stearns." Harvard Business School.

Rosenzweig, P. (2014). "The Bbenefits and Limits of Decision Models." McKinsey Quarterly Retrieved February 2014, from http://www.mckinsey.com/Insights/Strategy/The_benefits_and_limits_of_decision_models?cid=other-eml-alt-mkq-mck-oth-1402.

Rowe, G., G. Wright, et al. (1991). "Delphi: A Reevaluation of Research and Theory." Technological Forecasting and Social Change **39**(3): 235-251.

SEC. (2014). "Microcap Stock: A Guide for Investors." Retrieved January 3, 2014, 2015, from http://www.sec.gov/investor/pubs/microcapstock.htm.

Seijts, J. and P. Bigus (2012). "Sony PlayStation: Security Breach." Harvard Business School.

Siegel, P., J. Strawser, et al. (1998). Knowledge Acquisition and the Development of Decision Rules: Studying and Evaluating Internal Control Structures Applications of Fuzzy Sets and The Theory of Evidence to Accounting, II. New York, NY, JAI Press Inc.

Simon, H. (1966). The Shape of Automation for Men and Management. New York, NY Harper Torchbooks Academy Library

Smith, C. (2014). "It Turns Out Target Could Have Easily Prevented its Massive Security Breach." from http://bgr.com/2014/03/13/target-data-hack-how-it-happened/.

Smith, J. and T. Kida (1991). "Heuristics and Biases: Expertise and Task Realism in Auditing." Psychological Bulletin **109**(3): 472-489.

Srivastava, R. and G. Shafer (1992). "Belief-Function Formulas for Audit Risk." Accounting Review **67**(2): 249-283.

Stroh, P. (2005). "Enterprise Risk Management at Unitedhealth Group." Strategic Finance **87**(1): 26-35.

Taylor, F. (1911). Shop Management. Charleston, South Carolina, BiblioBazaar.

Turoff, M., M. Chumer, et al. (2004). "Assuring Homeland Security: Continuous Monitoring, Control and Assurance of Emergency Preparedness." Journal of Information Technology Theory and Application (JITTA) **6**(3): 24.

Turoff, M. and L. Plotnick (2012). The ISCRAM Future Threat Delphi: Nostradamus Revisited. ISCRAM, Vancouver, Canada.

VanHoose, D. (2007). "Assessing Banks' Cost of Complying with Basel II." from http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1066766_code545810.pdf?abstractid=1066766&mirid=1.

Vasarhelyi, M. (2005). Emerging CARLAB Work 10th World Continuous Auditing and Reporting Symposium. Rutgers Business School - Newark, New Jersey, USA.

Vasarhelyi, M., M. Alles, et al. (2004). "Principles of Analytic Monitoring for Continuous Assurance." Principles of analytic monitoring for continuous assurance **Vol. 1**.

Vasarhelyi, M., M. Alles, et al. (2012). "The Acceptance and Adoption of Continuous Auditing by Internal Auditors: A Micro Analysis." International Journal of Accounting Information Systems **13**(3): 267-281.

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

Vasarhelyi, M. and F. Halper (1991). "The Continuous Audit of Online Systems." Auditing **10**(1): 110-125.

Vasarhelyi, M., A. Kogan, et al. (2002). Would Continuous Auditing Have Prevented The Enron Mess? CPA Journal**:** 80.

Vasarhelyi, M., D. Lombardi, et al. (2010). "The Future of Audit: A Modified Delphi Approach." SSRN eLibrary.

Vasarhelyi, M., R. Teeter, et al. (2010). "Audit Education and the Real-Time Economy." Issues in Accounting Education **25**(3): 405-423.

Venkatesh, V., M. Morris, et al. (2003). "User Acceptance of Information Technology: Toward a Unified View." MIS Quarterly **27**(3): 425-478.

Viaene, S., R. A. Derrig, et al. (2002). "A Comparison of State-of-the-Art Classification Techniques for Expert Automobile Insurance Claim Fraud Detection." Journal of Risk & Insurance **69**(3): 373-421.

Wallace, W. (1984). "Internal Auditors Can Cut Outside CPA Costs." Harvard Business Review **62**(2): 16-20.

Warren, D. (2002). Data Mining As A Continuous Auditing Tool for "Soft Information": A Research Question 5th World Continuous Auditing and Reporting Symposium. Rutgers Business School - Newark, New Jersey, USA.

Warren, D. (2005). "Continuous Financial Controls Review Processes." Sarbanes-Oxley Compliance Journal.

Warren, D. and X. Parker (2003). Continuous Auditing: Potential for Internal Auditors. Altamonte Springs, FL, The Institute of Internal Auditors Research Foundation.

Weber, M. "Manual Accounting Versus Computerized Accounting." Retrieved November 11, 2011, from http://www.experience.com/alumnus/article?channel_id=accounting&source_page=breaking_in&article_id=article_1173385201144.

WebTrust.org. (2009). "Overview of Trust Services." Retrieved 9/8/2009, 2009, from http://www.webtrust.org/overview-of-trust-services/index.aspx.

Weick, K. (2001). Managing the Unexpected. San Francisco, CA, Jossey-Bass.

Whitehouse, T. (2010, November 30, 2010). "Whatever Happended to Continuous Auditing." Compliance Week, from http://www.complianceweek.com/article/6266?printable=1.

Wise, J. (2011). "What Really Happened Aboard Air France 447." Popular Mechanics **December 6, 2011**.

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

Yazid, A., M. Hussin, et al. (2011). "An Examination of Enterprise Risk Management (ERM) Practices among the Government-Linked Companies (GLCs) in Malaysia." International Business Research **4**(4).

Ye, H., S. Chen, et al. (2008). SOA-based Conceptual Model for Continuous Auditing: A Discussion. 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08), Hangzhou, China.

Zarowin, S. and W. Harding (2000). "Finally, Business Talks the Same Language." Journal of Accountancy **190**(2): 24-30.