ENTERPRISE RISK MANAGEMENT AT HIGHER EDUCATION INSTITUTIONS: HOW MANAGEMENT CONCEPTS SUPPORT ITS IMPLEMENTATION

By

Steven Christopher Deck

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland University College, in partial fulfillment
of the requirements for the degree of
Doctor of Management
2015

Advisory Committee:
Dr. Thomas J. Mierzwa
Dr. Denise A. Breckon

University of Maryland University College
The Graduate School

DOCTOR OF MANAGEMENT DEGREE

DISSERTATION APPROVAL FORM

DM candidate Steven Christopher Deck has completed all the necessary dissertation requirements of University of Maryland University College's Doctor of Management Program.

APPROVED:

Faculty Advisory Committee:

Thomas J. Mierzwa — 12/10/2015

Dr. Thomas J. Mierzwa — Date:

Denise A Breckon — 12/10/2015

Dr. Denise A. Breckon — Date:

ABSTRACT

Title of Dissertation: **ENTERPRISE RISK MANAGEMENT AT HIGHER EDUCATION INSTITUTIONS: HOW MANAGEMENT CONCEPTS SUPPORT ITS IMPLEMENTATION**

Steven Christopher Deck, Doctor of Management, 2015

Dissertation Directed By: **Dr. Thomas J. Mierzwa and Dr. Denise A. Breckon, Doctor of Management**

Higher education institutions are under increased pressure from government agencies, the public, and members of the campus community to manage risks. Traditionally, risk management responsibility has been delegated to individual operating units. This approach lacks an overarching strategy for managing risks and is being supplanted by an approach gaining favor in higher education for strategically managing risks now termed enterprise risk management. As a senior leadership lead initiative, enterprise risk management provides a comprehensive strategy for managing risks. However, since existing models originate from the business sector they lack guidance for implementing the approach in a higher education environment. The focus of this study examines why higher education institutions would adopt an enterprise risk management strategy and how critical success factors influence its implementation.

The central thesis of this study is that management concepts drawn from theory can enhance the implementation of enterprise risk management in higher education. To test this thesis, a conceptual framework for enterprise risk management implementation was derived from

a review of the theoretical literature on change management, decision making, and organizational learning. A systematic review methodology was employed to test the conceptual framework against findings from 55 research studies. Implications for practice include approaches for adopting enterprise risk management to improve organizational performance, clarifying its purpose, reflecting the culture of the institution in its design, assigning a program champion and cross-functional implementation team, assigning risk assessment methodologies based on the type of risk, and using an enterprise risk management approach to build organizational learning and resiliency. Theoretical implications include exploring how theories on change management, decisions making, and organizational learning can further extend research on this topic.

Keywords: *Change management, decision making, enterprise risk management, organizational learning, sensemaking, systematic review, resiliency, risk, risk management*

Acknowledgements

First, I would like to thank my advisory committee, Dr. Thomas Mierzwa and Dr. Denise Breckon, for their guidance during the dissertation journey. Their hard work and commitment to my growth as a scholar enabled me to complete my dissertation and grow intellectually. I would also like to thank the staff at the UMUC doctorate of management program, specifically Marina Caminis, Monica Graham, and Cindy Thomas, for their help on my research and ensuring that my doctoral experience was enjoyable. Last, to my cohort members, thanks for all your insight, support, and encouragement throughout this long and challenging process!

I would also like to acknowledge Dr. Roger Ward, Chief Accountability Officer, Vice President for Operations and Planning, and Vice Dean, Graduate School at the University of Maryland Baltimore for encouraging me to pursue my doctoral degree and his continued support throughout the process to achieve my doctorate degree.

I would like to thank my two puppies, Jenny and Trixie, who gladly took walks with me as pondered how to proceed with this dissertation. Last, and most importantly, I would like to thank my wife, Bonnie, for her patience and support as I fulfilled the demanding requirements of the doctor of management program. Her tolerance for deferring home improvements until after completing the program is appreciated!

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction and Management Problem

Risk is pervasive to conducting business. Consider any operation an organization performs: each requires identifying and managing the risks that can impede the execution of the operation. For example, production units must manage risks such as employee safety or the loss of a critical supplier or piece of equipment, human resource departments confront potential claims of unfair labor practices, and information technology groups must be alert to cyber threats. Moreover, organizations face external risks that arise due to advances in technology, changing economic and market conditions, and increased globalization. Higher education institutions (HEIs) are not exempt from these challenges and are under increased pressure from the government, public, and campus community to manage risks (The Advisory Board, 2008; University Risk Management and Insurance Association [URMIA], 2007). For example, HEIs must manage a wide range of risks in diverse areas such as safety and security, regulatory compliance, academic affairs, research, information technology, finance, human resources, and facilities management (Abraham, 2013). Furthermore, recent events such as hurricane Katrina, an economic downturn, and social issues such as sexual assault on campus and protest actions point out the importance of managing risk in higher education. Indeed, although the institution may survive such events, leadership may not. For example, both the Penn State Jerry Sandusky sexual abuse scandal in 2011 and the University of Missouri social protests of 2015 resulted in leadership changes at these institutions.

Traditionally, HEIs have deferred responsibility to managing risks to individual operating units at the institution. However, this approach lacks an overarching strategy for managing risks from an institutional perspective. The lack of a comprehensive risk management strategy leads to inconsistent risk tolerance levels, inefficient resource allocation for risk control activities, and a

lack of knowledge on how risk affects achieving the strategic objectives of the HEI. However, a method gaining favor in higher education for managing risks in a holistic manner is enterprise risk management (ERM). ERM is a senior leadership lead initiative that aims to integrate an organization's risk management practices in order to enhance the organization's ability to achieve its strategic objectives (The Committee of Sponsoring Organizations [COSO], 2004; Hoyt & Liebenberg, 2011). Indeed, in 2004 the Harvard Business Review listed ERM as a breakthrough management idea due to its ability to move beyond traditional risk management approaches that focus on managing risks in functional silos. Instead, ERM aspires to manage risks as a portfolio in order to capture the full range of risks and multiple interdependencies between them.

Hence, ERM has attracted attention from HEIs as a means to manage their risk in a comprehensive and strategic manner. However, existing ERM models originate from the business sector and were developed by practitioners from such fields as auditing, accounting, and insurance (Andersen, 2010). These frameworks emphasize hierarchal management structures, quantifying risk exposure, and control systems for managing risks. In addition, ERM is a relatively new management practice with limited empirical research on implementing the practice in complex organizational settings such as HEIs. Bromiley, McShane, Nair, and Rustambekov (2015) add that ERM frameworks fail to incorporate theories from the management sciences and assert, "Management scholars have particular methodological and theoretical bases that can complement ERM research in finance and accounting" (p. 273). Power (2007) adds that the risk management field has underexplored applying principle from the management sciences to improve the design of risk management processes. Further complicating matters, scholars have noted that adopting management approaches from the business sector is

viewed with skepticism by faculty at HEIs (Kezar, 2005; Meyer, 2007; Ramirez & Christensen, 2013; Taylor & Baines, 2012; Weller & van Gramberg, 2007). Therefore, HEIs face the challenge of introducing ERM frameworks that are undeveloped for complex organizational settings into an organizational culture already skeptical of new management approaches. In such a scenario, implementing ERM is unlikely to be successful. Consequently, the follow section outlines the context and dimensions of the management problem driving the central thesis for this study. Which is: concepts from management theory on change management, decision making, and organizational learning can explain and enhance strategies for implementing ERM in higher education.

Problem Statement

Albert Einstein once said, "the formulation of a problem is often more essential than its solution, which may be merely of mathematical or experimental skill" (as cited in Van de Ven, 2007, p. 70). According to Van de Ven (2007), grounding a research problem from the user's perspective—in this case leaders and risk management practitioners in higher education—offers the ability to understand the different dimensions and expressions of a problem. Grounding the problem in "reality" allows for a better appreciation of the problem's multiple dimensions, and aids in addressing the "what, where, when, why, and how" questions associated with the problem (Van de Ven, 2007, p. 77). This section defines three main dimensions of the research problem: the organizational environment at HEIs, traditional risk management, and enterprise risk management. The following discussion and analysis of the three dimensions of the study problem form the basis for the research question that guides this study.

Higher Education Institutions

The study proposes that HEIs are complex organizational settings that have multiple cultural dimensions. McDaniel (2007) explained that complex systems share five common characteristics: (a) multiple agents that have the capacity to adapt behavior based on new information, (b) nonlinear interactions, (c) self-organization that can result in new structures and forms of behavior, (d) the emergence of new and unpredictable systems, and (e) complex systems that coevolve with their environment (pp. 22–25). McDaniel (2007) further argued that traditional management approaches that focus on command, control, and planning require the ability to forecast future states; something impractical for complex systems. He thus proposed that complex systems require the application of management strategies based on sensemaking, learning, and improvisation. In his seminal work *How Colleges Work* (1988), Birnbaum noted several characteristics of HEIs consistent with those found in complex organizational settings. These include dual control systems (i.e., one for the administration and another for faculty); a lack of a quantifiable financial performance measure for the institution; unclear, shifting, and broad institutional missions; external funding that dilutes institutional control over faculty; decentralized decision making; and a lack of distinction between organizational levels (pp. 9–19). Indeed, for these reasons Birnbaum (1988) stated that "colleges and universities are the most paradoxical of organizations" (p. 3). HEIs therefore need to develop their ERM programs to be equipped to manage these issues.

Kezar (2001) stated that the context in which HEIs operate is unique and significantly different from private industry, necessitating the development of new concepts and methodologies for organizational change. Kezar continues that overlooking the different contextual factors found in higher education causes failures in analysis and strategy, and inhibits

the organization's ability to engage the stakeholders needed to effect change. Additionally, the University Risk Management and Insurance Association (URMIA; 2007) noted that HEIs operate in a complex and changing environment composed of societal, economic, and market forces. HEIs are also under pressure to transform their business practices. Drivers for this change include intense competition for faculty and student and funding; demands for increased efficiency and accountability; increased government and public scrutiny; new technologies that require substantial financial investment; increased entrepreneurial activity with private sector partners; expanding marketplace competition; and the proliferation of litigation (p. 7).

Moreover, the failure to manage risks properly can lead to events that challenge an organization's ability to meet critical objectives and jeopardize its survival. As McShane, Nair, and Rustambekov (2011) stated, "Managing risks has become a critical function for CEOs as organizational environments become increasingly turbulent and complex" (p. 653).

A survey by North Carolina State University and Protiviti (2015) identified the top risks executives perceive their organizations face as regulatory changes, economic conditions that restrict growth, attracting and retain talent, inability to identify risks, cyber threats, managing unexpected crisis, sustaining customer loyalty, resistance to change that restricts the ability adjust business models, and not meeting performance expectations (p. 7). Examples of top risks that are specific to HEIs include economic conditions, political change, financial stability, student enrollment, information technology and physical infrastructure, attracting and retaining talent, regulatory compliance, and building and protecting the institution's reputation (Abraham, 2013, pp. 12–13).

As a result, higher education has turned to ERM as a means to manage these risks and to address external stakeholder demands that institutions take proactive measures to manage risks.

Indeed, URMIA (2007) proposed that ERM can help HEIs sustain a competitive advantage, protect their reputation, respond effectively to adverse events, limit financial surprises, and improve how they manage resources (p. 7). Before discussing ERM, it is necessary to review how institutions have previously managed risks in order to understand the logic for HEI interest in ERM as a risk management strategy.

Traditional Risk Management

Traditional risk management is defined as "the process of making and implementing decisions that will minimize the adverse effects of accidental losses on an organization" (Baranoff, Harrington, & Niehaus, 2005, p. 1.5). This approach to risk management aims to identify potential loss exposures and examine the feasibility of various strategies to limit these exposures (Baranoff et al., 2005). Strategies utilized to manage risk fall into two categories: risk control and risk finance. According to Baranoff et al. there are six core risk control techniques: "avoidance, loss prevention, loss reduction, separation, duplication, and diversification" (p.2.19). As the name implies, avoidance simply means the organization does not take on an activity that exposes it to certain risks. Loss prevention and reduction involve actions to reduce the frequency and severity of losses from risks. Separation entails splitting up assets so they are not all exposed to the same risk. Duplication involves the use of redundant systems to prevent the shutdown of an operation or process. Finally, diversification spreads risk exposures over a range of operations, markets, or geographic regions (Baranoff et al., 2005, pp. 2.18–2.21). Examples of risk finance techniques include transfer methods, such as insurance, hold-harmless agreements, and hedging; while an example of retention is the self-funding of losses (Baranoff et al., 2005, pp. 2.21–2.23). Figure 1 illustrates the relationships between these different risk management techniques.

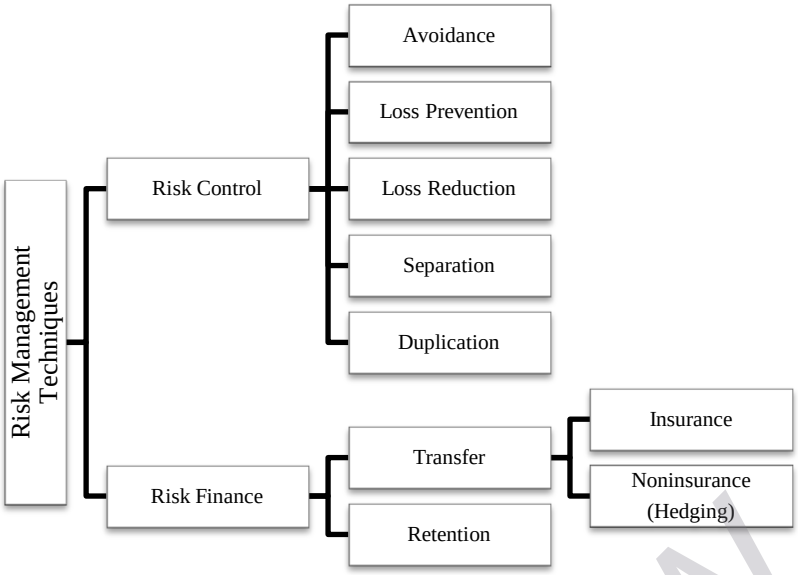

Figure 1. Risk management techniques. Reprinted from *Risk assessment* (1st ed.) by E. Baranoff, S. E. Harrington, & G. R. Niehaus (Eds.), 2005, p. 2.19. Copyright 2005 by The Institutes. Used with permission from The Institutes.

Traditional risk management techniques fail to address the full range of risk exposures an organization may face. Arena, Arnaboldi, and Azzone (2011) argued that a limit of traditional risk management is its tendency to manage risk categories separately. Traditional risk management functions have often been located in the accounting, financial, compliance, and internal auditor areas of organizations (Blaskovich & Taylor, 2011). Moreover, March and Shapira (1987) contended that theories on managerial perspectives of risk, such as classical decision theory, oversimplify human behavior and thus do not accurately explain how managers perceive risk. Brinkmann (2013) suggested that the complexity of modern risk combined with increased pressure to hold organizations accountable for their actions can lead to managers focusing on providing a defendable justification for their decisions concerning risk at the expense of using sound professional judgment. Accordingly, Brinkmann (2013) posited the need for "intelligent risk management" based on the following tenets: (a) control systems that are not

allowed to overburden managerial attention and innovation, (b) higher tolerance levels for disorganization and ambiguity in the risk management process, and (c) internal control systems that focus on generating usable knowledge and that are always challengeable (p. 578). ERM frameworks such as the one offered by COSO begin to address the three dimensions of intelligent risk management; however they require more insight on how to manage risk without stifling innovation, how to assess risks with high levels of ambiguity, and how to create actionable knowledge through the risk management process.

In sum, modern organizations face a wide range of complex risks that challenge their ability to meet mission-critical objectives. In addition, managing risk is more complicated in large institutions composed of multiple subunits that operate in a global, changing economy (Grabowski & Roberts, 1997). Consequently, scholars (e.g., Powers, 2007) have proposed that traditional approaches to risk management should be replaced by methods that position risk management as part of an organization's governance process, allowing for a more holistic view of the organization's risk exposure. ERM is such a strategy.

Enterprise Risk Management

In response, some organizations have adopted the integrative approach to risk management known as ERM. By integrating risk management into an organization's strategic decision-making processes and operations, ERM overcomes the limits of traditional risk management approaches that manage risk in "silos". ERM does this by positioning risk management as a senior leadership responsibility, assessing risk from an entity-wide perspective, aligning business strategies with risk tolerances levels, and integrating accountability for managing risk across the entity (COSO, 2004; Kimbrough & Componation, 2009; Kleffner, Lee, & McGannon, 2003; McShane, Nair, & Rustambekov, 2011).

There are several existing frameworks for ERM, including: the Casualty Actuarial Society ERM framework, the Committee of Sponsoring Organizations (COSO) ERM integrated framework, the International Organization for Standardization (ISO) 31,000 risk management framework and process, the Australian and New Zealand standard for risk management, and the Federation of European Risk Management Associations' risk management standard (Andersen, 2010; Kimbrough & Componation, 2009). These frameworks share similar risk management steps and highlight how ERM influences a broad range of activities and organizational levels (Kimbrough & Componation, 2009). Moreover, these frameworks portray ERM as a top-down, driven risk management approach (Andersen, 2010). This study employed the COSO ERM integrated framework since it is the most prevent model referenced in the reviewed ERM literature.

COSO was established in 1985 to address the increased incidence of fraudulent financial reporting. This initially resulted in COSO developing frameworks to improve financial reporting and compliance. COSO then published the ERM integrated framework in 2004, which is referenced by several U.S. and international standard-setting bodies (Landsittel & Rittenberg, 2010). The committee is composed of five sponsoring organizations: the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the Institute of Management Accountants. Its mission is "to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations" (Landsittel & Rittenberg, 2010, p. 457). The committee's composition and mission are especially important as they reveal the professional background of the

framework's developers and, subsequently, the challenges HEIs may have implementing a framework that relies heavily on internal controls and top-down management strategies.

> According to COSO (2004), enterprise risk management is
>
> a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting 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. (p. 4)

This definition outlines the following six key elements of ERM: (a) led by senior management, (b) integrated throughout the organization, (c) considers risk from a strategic perspective, (d) provides reasonable assurance of meeting an organization's goals, (e) identifies risks that affect the organization, and (f) manages risk based on the organization's risk appetite and tolerance level. In addition, COSO proposed four critical areas for establishing risk management objectives: (a) strategic objectives, which involve high-level goals and the mission of the organization; (b) operation objectives, which outline the efficient use of organizational resources; (c) objectives to meet an organization's reporting requirements; and (d) regulatory compliance objectives (p. 21). According to COSO (2004), organizations need to set objectives for managing risk at each organizational level to include the entity, divisional, business unit, and subsidiary levels of the organization (p. 23).

The COSO (2004) ERM framework is composed of eight interrelated components. These include: (a) the internal environment, such as the organization's risk management philosophy, ethical values, and the operating environment; (b) objectives that align with the organization's tolerance for risk; (c) the identification of internal and external events that present risks to the organization; (d) the assessment of events to determine the likelihood and impact risks may have