8-5-2011

Business Intelligence in Corporate Risk Management

Gunwoong Lee
Arizona State University, Gunwoong.Lee@asu.edu

Uday Kulkarni
Arizona State University, uday.kulkarni@asu.edu

Business Intelligence in Corporate Risk Management

Gunwoong Lee and Uday Kulkarni

Department of Information Systems
W. P. Carey School of Business
Arizona State University
Tempe, AZ 85287-4606
Gunwoong.Lee@asu.edu; Uday.Kulkarni@asu.edu

ABSTRACT

The academic literature and industrial reports have called for organizations to manage their corporate risks; however, there is still a lack of studies on effective risk management that take advantage of information technology (IT). Conventional IT-based internal controls allow organizations to build shareholders' confidence by ensuring transparency in internal business processes, but their capacity to effectively manage comprehensive organizational risks is limited. In this study, we introduce risk intelligence as an effective risk management method. By applying key properties of business intelligence (BI), risk intelligence can prepare organizations for a variety of severely disruptive events (including external risks) and empower them to take risks as a means to value creation. We explore the application of BI to various aspects of corporate risk management. Our analysis shows that risk intelligence can provide greater benefits to organizations by managing internal and external risks, improving the shock resilience before an event takes place, and supporting senior management's decision making through integrated scenario planning.

Keywords

Risk intelligence, internal control, risk management, internal risk, external risk.

> *"Organizations that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run, outperform those that are less so. Simply put, companies make money by taking intelligent risks and lose money by failing to manage risk intelligently"*
> Deloitte, 2007

1. INTRODUCTION

As noted in the above quote, effective corporate risk management has become a prominent factor in the modern business world and can contribute to a firm's competitive advantage. Risk management is generally regarded as the process of analyzing risks and determining how to best handle such risks. The importance of effective risk management in businesses and in corporate functions has been implicitly or explicitly acknowledged for many years. Recent financial corruption and business failures, such as the Enron and WorldCom scandals, have increased the demand for developing information systems (IS)

with capacity to deal with organizational risks in many global companies as well as in public sectors. Many companies have introduced internal control (IC)[1] in order to curtail internal risks to acceptable levels (more specifically, to comply with Section 404 of the Sarbanes-Oxley act of 2002). However, IC is not likely to be effective in managing comprehensive organizational risks for the following reasons. First, IC mainly focuses on detecting risky activities within an organization. Consequently, IC is vulnerable to external risks that are unexpected but happen regularly enough regardless of organizational activities. Second, IC cannot control currently occurring risks, making it hard for companies to response to the risks quickly. Third, the management of IC is restricted to the internal audit team. The detected internal risks are reported to the higher-level management without a comprehensive understanding of the organizational goals threatened by such risks.

In order to overcome these drawbacks of IC, our study introduces a new risk management method, i.e., risk intelligence (RI). RI is based on the key insights from business intelligence (BI) and its role in risk management is to assist an organization to raise the intelligence about risks it takes. That is, RI can be considered as a method that responds to corporate risks intelligently by learning how to deal with risks.

Although many industrial managers and researchers have argued that IC makes use of information technologies (IT) (Pearlson and Saunders 2006) and a BI infrastructure helps the company achieve financial-reporting compliance of the SOX act (Rogalski and Lin 2003), IC does not sufficiently utilize information technologies, specifically BI, in the process of risk management. Many companies have used information technologies for IC to gather large volumes of financial data into a financial database, to detect anomalies in the database, and to deliver reports to higher management. However, precise predictions and pattern analyses based on the historical data, use of real-time data for risk monitoring, and swift communications among all members throughout the organization is still under way. RI can assist a company in improving the risk management process by utilizing BI.

Several studies in finance, accounting, computer science, and information IS have been conducted on the benefits of IT based corporate internal control (Brown and Nasuti 2005; Stoel and Muhanna 2010), the value of risk management (Mackay and Moeller 2007), and the strategic uses of BI (Andriole 2006). However, to our knowledge, no study has examined how BI can be applied to corporate risk management or explained how RI enables companies to achieve a competitive advantage over rivals. Consequently, the lack of studies on RI makes it difficult to theorize its impact on risk management.

For the purpose of closing this research gap, our study examines how corporate risks are effectively managed by taking advantage of BI. The use of RI in corporate risk management provides greater benefits to companies by predicting a variety of potential risks effectively and responding to those risks more proactively as compared to IC. Consequently, this study attempts to answer the following research questions:

- How can business intelligence enhance the corporate risk management process?
- How can BI be used in corporate risk management?
- What are the benefits of risk intelligence (RI) in risk management?

[1] Under the Committee of Sponsoring Organizations (COSO) framework, internal control is broadly defined as "a process designed to provide reasonable assurance regarding the achievement of objective hindered by potential risks by assuring effectiveness and efficiency operations, reliability of financial reporting, and compliance with laws and regulations"

The remainder of this paper proceeds as follows. In section 2, we discuss the literature relevant to our present work. In section 3, we make comparisons between IC and RI. In section 4, we provide practical examples how RI can be applied to real world business problems and how it enhances the corporate risk management. We discuss the implications of our results in section 5.

2. LITERATURE REVIEW

Although research on the applications of business intelligence to risk management is just emerging, a large volume of literature in accounting, finance, and IS provides the groundwork for answering the research questions. We build on this literature to create new knowledge about BI in corporate risk management.

2.1. CORPORATE RISK MANAGEMENT

There is vast literature on enterprise risk management (ERM) based on financial asset portfolio and corporate internal control (IC) for managing risky activities in an organization. In finance and accounting studies, corporate risk management is mostly related to reducing potential risks of investments in risky assets (Barrese and Scordis 2004) and creating value under uncertainty through risk management (Mackay et al 2007). Internal control related studies in accounting and IS mostly focus on explaining how companies can manage internal risk (Ashbaugh-Skaife, Collins, Kinney, and Lafond 2009), determinants of internal control weaknesses (Doyle Ge, and MacVay 2007; Ge and McVay 2005), and successful compliance of SOX requirements by adopting IT (Chang, Wu, and Chang 2007; Hall and Liedtka 2007). Since the goal of internal control is to manage risk in an organization at a lower level (Griffiths 2006) and to enhance the shareholder trust based on reliable financial reporting (Coates 2007), the purpose of IC is to make organizations focus more on managing internal risky activities rather than on comprehensive corporate risks.

Comprehensive corporate risks arise not only from internal sources, but also from external sources. The extant literature has not fully addressed external risks because it is difficult to scientifically measure factors related to external risks. Moreover, the lower frequency of occurrence of external risks makes it difficult for researchers to draw generalized conclusions. Some studies have confirmed the existence of underlying external factors that affect organizations' goals, e.g., technology related problems (Singh 1997), political and geographical issues (Branner, Pavelin, and Porter 2006), and conflicts in partnerships, or third-party relationships (Sobel 2010). Our study explores how organizations can manage internal and external risks in an effective manner by using BI.

2.2. BUSINESS INTELLIGENCE

BI has been used as an umbrella term to describe concepts and methods to improve business decision-making by using an organization's data and information. BI includes the underlying architectures, analytical tools, applications, databases, and methodologies (Turban et al, 2010). BI's main objectives are to enable interactive and easy access to diverse data, and enable manipulation and transformation of these data with a decision-making focus. BI provides individual managers and organizations the ability to conduct analyses and perform actions. In addition, BI uses complex statistical and other mathematical models to discern interesting patterns for understanding associations between variables and make

predictions to create economic value. In this sense, BI is now widely adopted in the world of IT practice and has become an essential business capability (Waston and Wixom, 2007).

Many studies show how successful BI initiatives have been undertaken. Jourdan et al (2007) reveals that 59 out of 167 BI-related articles appearing in leading IS journals between 1997 and 2006 focused on how BI tools and technology are applied in the modern business practices and how these BI applications assist the organizations to achieve their strategic objectives: manufacturing companies (Houghton, El Sawy, Gray, Donegan, and Joshi 2004), airlines (Anders-Lehman, Watson, Wixom, and Hoffer 2004; Wixom, Watson, Reynolds, and Hoffer 2008), hotel chains (Piccoli and Applegate 2002), and entertainment industry (Watson and Volonino, 2007). Although several studies argue that BI supports IC and helps companies comply with the SOX act, in fact, the use of BI in the corporate internal control is still quite restricted. Companies have generally utilized IT for gathering data and sharing risk reports. Thus, the absence of intelligent risk management, including risk pattern analyses, predictions of potential risks, and real-time monitoring systems, makes the companies vulnerable to a large number of risks. Risk intelligence can be regarded as a BI application for ensuring safe, risk-averse business processes.

2.3. RISK INTELLIGENCE

There is still a lack of academic literature on risk intelligence although a large volume of industrial reports has shown the increased demand for studying RI (Deloitte 2007, KPMG 2009, SAS 2009). From this perspective, enlightened risk management not only considers the "bad things" that could happen from taking risks, but also the "good things" that might be linked to success so the organization can capitalize on opportunities (Wagner and Layton 2007). In this regard, Apgar (2006) defines risk intelligence as an individual or organizational ability to weigh risks effectively. It involves classifying, characterizing, and calculating threats, perceiving relationships, learning quickly, storing, retrieving, and acting upon relevant information, communicating effectively, and adjusting to new circumstances. The nature of risk is seemingly unpredictable and uncontrollable, but risk could be manageable through this intelligent risk management process. Apgar also explains and provides methods that evaluate the organization's risk intelligence (risk IQ). He suggests 5 measures to assess risk intelligence capability: amount of related experience (frequency), relevance of a typical experience (relevance), surprise element of the experience (impact), diversity of experiences (diversity), and record keeping (tracking). A high score on these measures puts an organization in a better position compared to others to reach accurate judgments for risks. However, the important questions about the effectiveness of risk management and its applications in the real-world businesses remain to be studied.

3. RISK INTELLIGENCE AND BI

ISO defines risk as "a combination of the probability of an event and its consequences" (ISO/IEC Guide 73: 2002). For organizations, a risk is a group of circumstances that hinders a company from achieving its objectives. Risk intelligence adapts key insights of BI to enhance an organization's ability to deal with comprehensive risks – internal and external. We show how RI can improve an organization's risk resilience by comparing it to conventional IT-based internal control.

3.1 INTERNAL RISKS AND EXTERNAL RISKS

Risks can be broadly categorized as internal risks that arise from inappropriate business activities within an organization and external risks that are outside the control of a business. They are unexpected but occur regularly and, therefore, need to be mitigated.

Table 1 shows three categories of internal risks with examples. Operational risks occur from inefficient use of resources such as excessive expenses compared to prior years. Compliance-related risks occur when employees do not follow applicable rules and regulations. Fraud is a risk incurred by employees' intentional misconducts designed to evade detection.

Operation	Compliance	Fraud
Excessive expenses compared to budgets	Inappropriate promotion	Use of corporate credit card during vacation

Table 1. Categories of Internal Risks

The external risks mainly originate from external circumstances and, therefore, they are generally hard to identify and predict. Table 2 shows several examples of external risks categorized according their properties. The common property of the external risks is that they generally occur without adequate forewarning and, hence, they are not detected until substantial damage is done. Furthermore, the absence of regulations and laws related to external risks makes it hard for organizations to prepare and respond to them.

Natural	Technological	Economic	Political	Man-made Disasters
- Influenza - Hurricane - Earthquake	- Data privacy - Computer virus - Hacking - IT security breaches	- Market Instability - Currency crises - Recession	- Terrorism - War	- Hazardous waste - Industrial accidents

Table 2. Categories of External Risks

3.2. COMPARISONS BETWEEN INTERNAL CONTROL AND RISK INTELLIGENCE

The use of RI offers a number of benefits in corporate risk management when compared to IC. Table 3 presents the main differences between these two risk management methods on several important aspects.

	Internal Control	Risk Intelligence
Objective	Control internal risks Build shareholder's confidence	Prevent and respond to risks quickly Take risks as a chance to value creation
Scope	Internal risk	Internal and external risks
Risk Assessment	Monetary impact, Frequency	(In)direct impact, Recovery cost
Timeframe	Present	Past, Present, Future
Monitoring	Continuous monitoring	Real-time monitoring
Response	Taking corrective actions and Compensating for damages	Reconfiguration of business process
Management	Managed by audit team	Managed by senior management

Table 3. Comparisons between IC and RI

***Objective*:** The main difference between IT-based internal control and risk intelligence originates from their objectives. While the main objective of IC is to control internal risks and build shareholders' confidence through reliable financial reporting, the goal of RI is to improve the ability to accurately estimate probabilities of potentially risky activities in all areas of business, that may lead to disruptions that have an enterprise-wide impact. This fundamental difference influences the organization's approach to the management of corporate risk. IC mainly focuses on detecting risky activities within an organization and limiting them to acceptable levels (Griffiths, 2006). Meanwhile, the essence of the RI approach is to use "intelligent" techniques to predict potential corporate risks, to improve shock resilience *before* an event takes place, and to utilize risks as an opportunity for value creation (Deloitte, 2010).

***Scope*:** The scope of the risk that each approach covers also distinguishes between the two methods. IC focuses on managing only the internal risks. Thus, companies that rely only on IC are vulnerable to comprehensive corporate risks that occur from uncontrollable external circumstances. By contrast, RI can include controls for risk that arise from internal and external sources. External risks can be controlled by systematically detecting patterns that have led to prior occurrences of risky events.

Risk Assessment: An internal audit team generally prioritizes a risk according to its monetary impact and its frequency. However, this measurement is limited to internal risky activities. For external risks such as natural disasters or technological mishaps, the monetary impact and frequency of risks cannot be accurately evaluated. Such risks are rare but they cause significant monetary losses by disrupting inside and outside business processes. RI overcomes the limited risk assessment capabilities of IC by including comprehensive risk measurements for *direct impact, indirect impact* and *recovery* via comprehensive data analysis. *Direct impact* refers to the extent to which a risk would affect the organization's resources in the short run, such as physical damage, loss of resources, absenteeism of employees, and regulatory penalties. *Indirect impact* refers to the extent to which the risk would affect the organization's long term prospects including impact on market share, reputation, customer relationships, etc. *Recovery* refers to the monetary costs and the time it takes to restore the company's operations to a state they would have been in the absence of the risky event.

***Timeframe*:** While IC detects only current risky activities and explains how they occur, RI provides historical, current, and predictive views of corporate risks for managing them. RI can learn from past risky events whose causes have been established after their occurrence. RI can further build cumulative knowledge by analyzing such events and responses. RI can also detect current risky activities based on historical risk information and evaluate them before taking action. Furthermore, learning from the past and the present risk management process, RI can predict and prepare for responding to potential risks in the future.

***Monitoring*:** In conventional IC, the internal audit team continuously monitors activities according to pre-determined risk priorities. The investigations are restricted to activities or transactions that seem abnormal, but have already occurred. For example, the audit team cannot prevent or reverse inappropriate transactions involving unauthorized use of corporate credit card instantly. In contrast, RI can use business intelligence to build a repository of patterns of activities and transactions leading to known risks. Using real-time data feeds, the company can prevent currently occurring risks by comparing them with the anomalous patterns. Such a monitoring process can be made part of daily business operations across the organization and may not be restricted to the internal audit team's span of control.

***Response*:** While responding to violations, IC concentrates on taking corrective actions to alleviate the impact of irregularities and noncompliance of procedures. RI, on the other hand, allows the organization to act according to contingency plans - integrated scenarios involving interconnected business processes - to recover from predicted risks. For example, a natural disaster such as a hurricane could have significant effects on the organization. In such a crisis, for instance, companies may experience a high level of absenteeism and an internal system failure throughout the organization. A company that uses risk intelligence will have established contingency plans to enable work to be performed from remote locations using back-up servers and systems to maintain business continuity for extended periods of time.

***Management*:** Senior management and internal audit team generally have different viewpoints of the risks. The management of IC is limited to the internal audit team. The audit team may not identify corporate risks other than financial reporting and, even if they do, may selectively report the detected risks to higher management based on their limited view. Thus, the reported risks or violations may inadvertently exclude matters that are critical to the enterprise. In the RI based risk management environment, a broader set of functions participates in the reporting and detecting process and the role of senior management is more pronounced. RI assists executives in evaluating the upstream and downstream impact of the risks on the company's value chain and to respond to the risks with long-term solutions based on organizational priorities. Thus, all members throughout the company experience a more transparent risk management process.

4. RISK INTELLIGENT PROCESS AND EXAMPLE

In this section, we describe the risk intelligence process with the help of a comprehensive example. By comparing with the general process of internal control, we highlight the enhancements in corporate risk management through RI.

The example describes the RI process in a company, ABC bank, facing potential technological risks: system hacking, IT security breach, and data privacy. Generally, these technological risks occur without warning, and therefore the events are not detected until the damage is done. Thus, without prudent preparations for these potential risks, the company may confront not only the theft of sensitive customer data such as the usernames, passwords, and account numbers, but also classified company information such as new project plans and confidential documents such as employee annual performance reviews. Furthermore, if this company's customer systems (e.g., online banking systems) are down due to system abnormalities, customers cannot transact instantly leading to significant losses.

Even though internal control may prevent the risks that occur within a company such as customer data leakages by insiders, the risks from the outside of internal business process may not be manageable with only IC. In this regard, RI provides the company with more effective risk management by allowing correct predictions based on historical information about technological risks, real-time information from monitoring systems for detecting the potential risks, responses to risks based on an integrated pre-planned scenario, and immediate communications throughout the company. Figure 1 depicts the risk intelligence process.

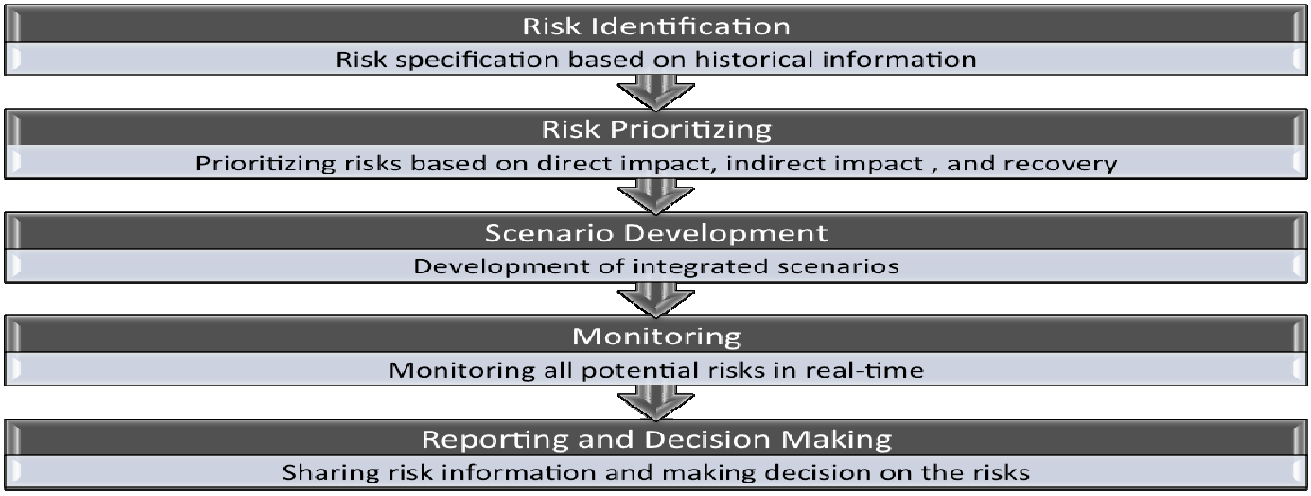

Figure 1. The Process of Risk Intelligence

Risk Identification: While IC recognizes and specifies potential risks according to related regulations and laws, the identification essentially happens after the events have occurred. By contrast, RI identifies the sources and patterns of the risks based on information and results from the risk analytics. For example, the bank specifies potential technological risks and identifies the patterns of the risks. The key in this step is to recognize the sources and properties of the technical risks by observing historical information about the risks or information from own or other companies (partners) who had similar risk experiences. Historical information on previously occurred system hackings and data privacy events enables the bank to learn when these technical risks generally took place and how insiders or unauthorized outsiders accessed the banking systems.

Risk Prioritizing: By prioritizing the risks using IC, the company is able to recognize which risks are most critical and to rate risks by their influence on the company. As we discussed in Section 3, in IC, the priority level of a risk is generally evaluated by its monetary impact and frequency. On the other hand, risk assessment using RI includes comprehensive measures for the consequences of the risk. In terms of *direct impact*, the system hackings and IT security breaches would lead to temporary or longer-lasting banking system unavailability, customer information leakage, transaction failures, and/or business data loss. As for the *indirect impact,* the company may lose loyal customers (or customers' confidence) and experience loss of market share. Regarding *recovery*, the technical weaknesses may take significant time and costs to get back to the point before the crisis occurred. Losses due to all of the above would be systematically estimated prior to the crisis while prioritizing risks in the RI process and appropriate resources would be dedicated for recovery.

Scenario Development: Once the risks have been analyzed, the company develops a scenario describing how to handle the high priority risks and to put in place the required actions that prevent the risk occurrences and minimize the impact of damages. Although, in the IC process, the internal audit team develops back-up plans for the highly probable risks, these plans are generally restricted to vouching and tracking the violations. Therefore, with this limited risk plan the bank is not be able to take proactive action before the security related incident surfaces. Meanwhile, based on the accurate predictions of potential technological risks, RI enables the company to build an integrated scenario that reconfigures all business processes affected by this technological threat. For example, if the bank confronts a high probability of online customer system downtimes due to system hackings, they can use separate servers or mirror sites before the hacking attempts are successful.

Monitoring: For the risk monitoring process of IC, internal audit teams generally control risk according to its priority-level, (e.g., Continuous Controls Monitoring). However, this does not ensure the prevention or avoidance of currently occurring events. With most security related technological threats, prevention is more critical than detection. In this regard, RI assists the company in predicting and taking appropriate measures to offset the risks instantly by monitoring all potential risks and computing the likelihood of risk occurrences in real-time. For instance, banks are one of the main targets of denial-of-service (DoS) attacks (e.g., the National Bank of Georgia in 2008 and PostFinance in 2010). Since DoS attacks can be perpetrated in multiple different ways, the sources are hardly ever identified. Hence, the best way to mitigate damages is to discover the symptoms of DoS attacks instantly and to block the attacks in advance, instead of tracking the origins. The intelligent monitoring process would equip the company to notice early signs of attacks immediately so that the bank how can respond to those threats before they strike in full force.

Reporting and Decision Making: Unlike the reporting process in IC, the detected risks and highly probable risks are directly reported to the senior management without filtering from the internal audit team. The senior managers and top decision makers may monitor the information on the company's overall risk exposure through a risk dashboard. Thus, if there is a high probability of system hackings, the senior executives can determine how to proactively respond to the risks according to the precise prediction and an integrated scenario. Consequently, the decision to handle the risks will be transmitted to the required functions of the bank stated in the scenario and each function will take appropriate measures according to its back-up plans. Also, because the long-term consequences of the security breach are predicted in advance, appropriate resource would also be released (e.g., loss compensation to customers, mediators and legal resources for anticipated claims, etc.).

As can be seen, the risk management based on RI enables the company to promptly respond to the crisis through a comprehensive risk management process. Moreover, as a result of RI, the bank can have new revenue streams from managing the risks properly. If the system hacking were prevalent throughout the industry, an RI-based company will have an opportunity to not only increase customer confidence, but also attract more customers by providing appealing vigilant risk management capabilities.

5. CONCLUSION

Our research has attempted to prescribe a systematic application of business intelligence to corporate risk management by suggesting benefits of risk intelligence compared to the conventional IT-based risk management approach. Our study indicates that organizations may not only have an opportunity to make their business processes suitable for managing risks, but also to alleviate damages incurred by internal and external risks through intelligent risk management.

From an industrial perspective, our study not only suggests better utilization of the BI infrastructure for risk management (e.g., real-time monitoring, risk analytics, risk dashboard), but also provides a guideline for effective risk management based on BI. Many companies has actively introduced risk management methods built on BI, but the role of BI is typically restricted to aggregate risk data and monitoring pre-determined risky activities, which means that companies are still susceptible to new and variant risks. In this context, the examination of effective BI use for corporate risk management and its benefits in improving risk resilience is valuable.

This study contributes to the extant literature both on risk management and on business practices. First, from an academic perspective, our research creates new knowledge about intelligent risk management

by suggesting a BI-based RI framework. The field of BI-based risk management is new and consequently has a diverse set of research issues. The growing demand for effective corporate risk management will need researchers to conduct studies on specific aspects of the framework presented in this paper. For example, while this study has concentrated on the use of key BI concepts for risk management, it might be interesting to examine how RI affects an organization's performance. To the extent that a firm can respond quickly to risks and minimize damage by using RI, it will have a significant competitive advantage over its competitors. Moreover, it would be worthwhile to examine how RI can help organizations recognize learnable and reward-able risks from a myriad of risks. This ability can help RI-enlightened business generate new revenue streams by taking truly "calculated" risks.

REFERENCES

1. Anderson-Lehman, R., Watson, H., Wixom, B., and Hoffer, J. (2004) Continental Airlines Flies High with Real-Time Business Intelligence, *MIS Quarterly Executive*, 3, 4, 163-176.
2. Andriole, S. J. (2006) The Collaborate/Integrate Business Technology Strategy, *Communications of the ACM*, 49, 5, 85–90.
3. Apgar, D. (2006) Risk Intelligence: Learning to Manage What We Don't Know, Harvard Business School Press.
4. Ashbaugh-Skaife, H., Collins, D., Kinney, W., and LaFond, R. (2009) The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity, *Journal of Accounting Research*, 47, 1, 1-43.
5. Barrese, J. and Scordis, N. (2004) Corporate Risk Management, *Review of Business*, 24, 29-34.
6. Branner, S., Pavelin, P., and Porter, L. (2006) Corporate Social Performance and Geographical Diversification, *Journal of Business Research*, 59, 9, 1025-1034.
7. Brown, W. and Nasuti, F. (2005) What ERP Systems Can Tell Us about Sarbanes-Oxley, *Information Management and Computer Security Journal: Information Management & Computer Security*, 13, 4, 311-327.
8. Chang, S., Wu, C., and Chang, I. (2009) The Development of a Computer Auditing Systems Sufficient for Sarbanes-Oxley Section 404 – A Study if The Purchasing and Expenditure Cycle of The ERP System, *Information System Management*, 25, 3, 211-229.
9. Coates, J. (2007) The Goals and Promise of the Sarbanes-Oxley Act, *Journal of Economic Perspectives*, 21, 1, 91-116.
10. Deloitte. (2010) Risk Intelligence Enterprise Management: Running the Risk Intelligence, Available: http://www.deloitte.com(Current Feb. 27, 2011)
11. Ge, W. and McVay, S. (2005) The Disclosure of Material Weaknesses after the Sarbanes Oxley Act, *Accounting Horizons*, 19, 3, 37-158.
12. Griffiths, D. (2006) Risk Based Internal Auditing: An Introduction, Available: http://www.internalaudit.biz
13. Hall, J. and Liedtka, S. (2007) The Sarbanes-Oxley Act: Implications for Large-Scale IT Outsourcing, *Communications of The ACM*, 50, 3, 95-100.
14. Houghton, R., El Sawy, O., Gray, P., Donegan, C., and Joshi, A. (2004) Vigilant Information Systems For Managing Enterprises in Dynamic Supply Chains: Real-Time Dashboards At Western Digital, *MIS Quarterly Executive*, 3, 1, 19-35.

15. International Organization for Standardization (ISO), Risk management -Vocabulary - Guidelines for use in standards, ISO/IEC Guide 73: 2002.
16. Jourdan, Z., Rainer, K., and Marshall T. (2008) Business Intelligence: An Analysis of the Literature, *Information Systems Management*, 25, 2, 121-131.
17. KPMG(2009) KPMG Corporate Intelligence, Available: http://www.kpmg.com(Current Feb. 27, 2011)
18. Mackay, P. and Moeller, S. (2007) The Value of Corporate Risk Management, *The Journal of Finance*, 62, 3, 1379-1419.
19. Pearlson, K. and Saunders, C. (2006) Managing & Using Information Systems: A Strategic Approach, 3rd Edition, Hoboken, New Jersey: Wiley & Sons, Inc.
20. Piccoli, G. and Applegate, L. (2003) Wyndham International: Forecasting High-Touch with High-Tech, Harvard Business School Case Study, 1-42.
21. Rogalski, S. and Lin, F. (2003) The Impact of the Sarbanes-Oxley Act on Financial Reporting & 360-Degree Insight, *DM Review*, 44
22. Singh, K. (1997) The Impact of Technological Complexity and Interfirm Cooperation on Business Survival, *Academy of Management Journa*l, 40, 2, 339–367.
23. SAS(2009) SAS Risk Intelligence Offerings, Available: http://www.sas.com(Current Feb. 27, 2011)
24. Sobel, P. (2010) Is Everyone Anticipating Risk?, *The Internal Auditor*, 67, 1, 59.
25. Stoel, M. and Muhanna, W. (2010) IT Internal Control Weaknesses and Firm Performance: An Organizational Liability Lens, Miami University and Ohio State University, Working Paper.