“Integration of enterprise risk management and management control system: based on a case study”

AUTHORS	Ilhang Shin https://orcid.org/0000-0003-1221-4519 Sorah Park https://orcid.org/0000-0003-3014-7065

ARTICLE INFO	Ilhang Shin and Sorah Park (2017). Integration of enterprise risk management and management control system: based on a case study. *Investment Management and Financial Innovations*, *14*(1), 19-26. doi:10.21511/imfi.14(1).2017.02
DOI	http://dx.doi.org/10.21511/imfi.14(1).2017.02
RELEASED ON	Friday, 31 March 2017

JOURNAL	"Investment Management and Financial Innovations"
ISSN PRINT	1810-4967
ISSN ONLINE	1812-9358
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
17	3	3

Ilhang Shin (South Korea), Sorah Park (South Korea)

Integration of enterprise risk management and management control system: based on a case study

Abstract

This paper aims to discuss the concepts and methodological issues of enterprise risk management (ERM). The case study of company A shows that ERM has been implemented and integrated with management control as a means of monitoring its subsidiaries. First, ERM system was implemented through comprehensive review of corporate risk policies, risk management processes, roles and responsibilities, and risk culture. Second, company A integrated ERM with the existing management control system in order to evaluate the risk underlying the current management activities. Finally, ERM implementation was expanded to all subsidiaries so that each business unit would be delegated for its own risk management. This paper provides insight on the process how group-level internal auditors can use ERM as a tool to manage risk of subsidiaries, thereby filling the gap between academic research and practice. This successful ERM adoption case can be used as a guideline for other organizations, which plan to adopt ERM with reduced costs and improved processes.

Keywords: risk management, enterprise risk management (ERM), internal audit, management control system.
JEL Classification: M41, E3.

Introduction

Bankruptcies of Enron and Worldcom in early 2000s proved that companies which achieved short-term growth and profitability through fraudulent accounting and falsehood contracting ultimately failed. Subprime mortgage scandal in 2006 and global financial crisis in 2008 also showed that companies are exposed to profile of unpredictable risks and uncertainty in financial markets. Since the frequency of risk and its harmful impact on corporate performance increased globally, regulatory agencies have enacted corporate risk management in many countries. U.S. Securities Exchange Commission (SEC) requires risk disclosures in 10-K and 10-Q filings, and accordingly U.S. listed companies disclose their risk exposure and risk management activities in their annual and quarterly reports. In Germany, Federal Ministry of Justice requires risk management system based on the business control and transparency regulation enacted in 1998 (KonTraG, Gesetz zur Kontrolle und Transparenz), and companies have to report risk management activities to regulatory agency on regular basis[1]. Also, since 2009, credit rating agencies such as S&P and Fitch have considered whether risk management system has been adopted by organization for corporate ratings. In addition, "risk & crisis management" has been included as one of major factors in Dow Jones Sustainability Index (DJSI)[2].

Therefore, the role of internal controls within organization is expanding from ex-post uncovering non-compliance to managing risk proactively and enhancing firm value. Traditional function of internal control has been to be a policeman assuring compliance with legal policies and regulations (Flesher and Zarzeski, 2002). However, recent trend is to be an internal consultant who identifies harmful issues and risk that may hinder achieving goals and improves risk management and auditing (McNamee and Selim, 1998; Weidenmier and Ramamoorti, 2006). This implies that the role of internal auditors is changed from monitoring risk of individual department to leading proactive risk management at enterprise level.

Enterprise risk management (ERM) has emerged as a paradigm for managing various kinds of risks faced by organizations, and the trend is to focus on its role in improving risk management and ultimately enterprise value. ERM is designed to improve the board and executives' oversight of risks. Such paradigm is a big improvement from the existing risk management practice, which has limitations in responding to dramatic change in business environment, since individual department has different management strategies and repeating inputs toward the same risk, resulting in low efficiency in risk management.

Ilhang Shin, Ph.D., Assistant Professor of Accounting, College of Commerce, Chonbuk National University, Korea.
Sorah Park, Ph.D., Assistant Professor of Accounting, Ewha School of Business, Ewha Womans University, Korea.

[1] Besides, Toronto Stock Exchange encourages the systematic internal control activities including risk evaluation and responses in the DeyReport (1994).

[2] For DJSI, the evaluation of ERM is included in the assessment criteria, specifically "Risk & Crisis Management" category. Companies are asked to answer not just "yes" or "no", but the details including data of recent few years in questionnaire. The questions are about the role of Chief Risk Officer (CRO) among top executive, his/her job description and responsibilities, risk analysis, risk correlations, sensitivity test, stress test, response strategy, crisis management, etc. The presence of risk officer and contingency plans are crucial factors for a company's sustainable growth.

The Committee of Sponsoring Organizations for the Treadway Commission (COSO), which was launched in order to improve monitoring misrepresentation in financial reporting, has updated the Internal Control Integrated Framework in 2004, originally published in 1992 and widely used by listed corporations for purposes of compliance with Sarbanes-Oxley Act. According to the Wall Street Journal[3], the update expands the scope of the framework and increases the level of detail of ERM, potentially expanding its utility beyond external financial reporting. Integrated risk management refers to implementation of three fundamental risk management objectives: modifying operations, using targeted financial instruments, and adjusting capital structure (Meulbroek, 2002). Meulbroek (2002) defines ERM as a framework intended to help managers to design a value-maximizing, enterprise-wide corporate risk management system via aggregation of all risks faced by the firm into a net exposure and coordinated use of these three risk management techniques.

This paper intends to discuss concepts and methodological issues of ERM, which is considered an extension of internal audit function. In doing so, this paper will have academic and practical implications by explaining factors that are related to successful ERM implementation and how to evaluate ERM capability. Also, internal audit practices can be strengthened by implementing internal control improvement strategies based on ERM. Moreover, external auditors' understanding of ERM system within audited corporations will be increased so that ERM infrastructure can be utilized for efficient and effective auditing.

Furthermore, we study the case of company A in which ERM has been implemented as a means to integrate with management control and to increase firm value by monitoring its subsidiaries. This paper provides insights on the process how group-level internal auditor can use ERM as a tool to manage risk of subsidiaries, thereby fills the gap between academic research and practice. There could be some areas within conglomerates (for example, "chaebol" in Korea), where group-level monitoring or control cannot reach. Reliance upon key performance indicator (KPI), a measure to quantify financial risks, or internal control has limitations in managing enterprise-level risk. Also, autonomic control by subsidiaries has the similar limitation. Hence, this paper presents the successful ERM adoption case that can be used as a guideline for other organizations, which plan to adopt ERM in the future with reduced costs and improved processes.

1. Concepts and methodological issues of ERM implementation

Corporate control itself does not create value. Rather, it is a mechanism that can be used to manage an entity's objective, strategies, and risk. According to the Institute of Internal Auditors, internal control is a series of rules and procedures, which are undertaken by management in order to improve risk management and the capability to achieve the objective of organization.

Among various definitions of ERM in the literature, ERM is usually defined as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO, 2004, p. 2)"[4]. Namely, ERM allows companies to identify and evaluate all types of risk, including financial risk and catastrophes that have been individually managed and external market condition and business risk, so that they can have a more systematic and integrated risk management process and increase the firm value.

According to COSO (2004), ERM system should be designed to achieve three main objectives: (1) strategy: high-level goals that support the organization's missions, (2) operations: effective and efficient use of a firm's resources, (3) financial reporting: reliability of reporting system, (4) compliance: organizational compliance with applicable laws and regulations. As now, the range of SOA internal control over financial reporting and internal audit system is limited to one of them, which is reliability of financial reporting. However, based on the analysis of company A, only 14% of workforce has been dedicated to tasks related to reliability of financial reporting.

COSO (2004) conceptualized the ERM frame work by integrating COSO I (1992) internal control model and risk management process. First, internal control system is expanded to ERM frame work. Second, entity objectives have been modified to strategy, operations, reporting and compliance.

[3] http://blogs.wsj.com/riskandcompliance/2013/05/14/updated-coso-framework-effective-today/.

[4] Definition of ERM was also provided by Casualty Actuarial Society (CAS) in 2003. The Casualty Actuarial Society (CAS) defined ERM as "the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders".

Third, three new ERM components (control activities, information and communication, monitoring) have been added to existing components (internal environment, objective setting, event identification, risk assessment, risk response). According to the updated framework, ERM can be viewed as a part of management control infrastructure to achieve corporate goals. For ERM to operate effectively as management control infrastructure, it is necessary to implement ERM system with comprehensive consideration of risk policy, management process, role and responsibility clarification, support system and risk culture.

There are five core steps for successful implementation of ERM as a management control infrastructure. First, management should analyze the needs for ERM in each subsidiary. In doing so, current risk management practice should be assessed in order to draw ERM-related issues. Second step is to identify/evaluate all potential risk of subsidiaries and select risk that needs to be managed with priority at enterprise level. Third, management should, then, take corrective actions to improve risk management. For this, they need to study the causes and effects of each priority risk, select KPI based on their importance, and quantify the likelihoods. Fourth step is to implement risk management system. This assures risk management system to utilize the risk profile and KRI list, which have been completed from the previous steps and to clarify the official role and responsibility of each team in the ERM process. The last step is the follow-up oversight on ERM system in order to monitor the effectiveness of ERM system that has been implemented as the management control system in step 4. In sum, step1~step3 are in place to come up with risk at priority and KRI at subsidiary level and step4~step5 are used to implement the management control system based on the risk and KRI deducted from step1~step3.

2. Relationship between ERM, internal control and internal audit

Due to large corporate scandals and accounting frauds such as Enron and Worldcom, the United States enacted the Sarbanes-Oxley Act in 2002 to enhance corporate transparency. At similar time, Korea amended the laws on corporate accounting to increase the transparency of after the 1997-98 Asian financial crises. One of key issues in these accounting regulations is to enhance internal control in the financial reporting and disclosure procedures.

In order to fully understand the background of such accounting regulations, it is necessary to understand the internal control. According to COSO Report[5] (which is considered the internal control standards in general), internal control is the process undertaken by board of directors, management and other members in order to achieve the following three goals: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, (3) compliance with applicable laws and regulations (COSO, 1992). COSO Framework defines the five elements of internal control as follows: (1) control environment, (2) risk assessment, (3) information and communications, (4) control activity, and (5) monitoring. Among these elements, control activity is specified at task level and the rest are specified at enterprise level.

Continuous internal auditing system supports the monitoring element of internal control. The main subject of monitoring is other internal control elements, more importantly, the effectiveness of control activity. In the case we study in this paper (a manufacturing company A), continuous monitoring system is used to oversee the following control activities in COSO Report: review & report on exceptional events, authorization by superior management, system configuration, processing consistent information, system access authority, system interface, segregation of duties[6].

Figure 1 shows the relationship between internal control, Korean SOX and continuous auditing system based on the COSO Framework. When viewing internal control from its objectives, Korean SOX is the internal control to enhance reliability of financial reporting. Continuous auditing system is the monitoring element of internal control of COSO Framework, which is monitoring the other internal control elements and, therefore, increases effectiveness and efficiency of internal control system. For companies, continuous auditing system could be considered an effective tool that supports internal accounting regulations such as SOX, as a part of compliance.

[5] In 1992, COSO Report (Internal Control – Integrated Framework) presents the tool for companies to conceptualize internal control system and evaluate the internal control system for future improvement. Since then, manycompanies in the U.S. use the COSO Framework as a guideline for evaluating internal control system. There is no legislation on definitions of internal control, but this COSO Framework has been considered the global standard of internal control.

[6] For example, continuous monitoring scenario such as "delayed/undelayed purchase orders due to purchaser master" aims to monitor the one of control activities "system configuration". If company A sets the system configuration to 'delay' for specific purchasers in ERP system module, the purchase order made by these companies cannot be processed. By doing so, the risk of trading with inappropriate purchasers will decrease, thereby enhancing internal control.

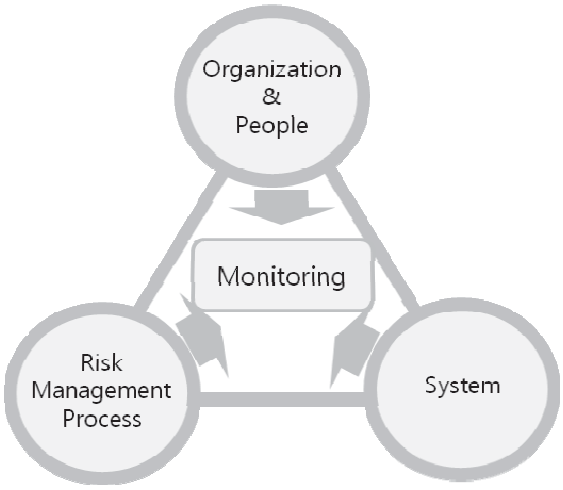

Fig. 1. ERM as a management control infrastructure

2.1. Integrating internal control and ERM. Traditional internal control/audit system has a compliance focus, whereas ERM takes a strategic approach voluntarily introduced by management's needs. Specific aim of traditional internal audit system is to enhance reliability of financial reporting, to comply with external audit regulations and SEC regulations and to evaluate responses of CEO, CFO and auditors. Point of focus includes control focus on financial reporting risk and assurance of control process for reliable financial information. On the contrary, ERM aims to manage the portfolio of risks that face organizations, ex ante risk management. The purpose of ERM is much broader, managing ex ante risk faced by organization and managing main corporate areas such as corporate strategy, long-term projects, and large-scale investments. Also, the range extends to strategic goals, efficient and effective operations, reliable financial reporting, and compliance. Point of focus is holistic risk analysis and evaluation.

Prior research on internal control has shown that effective internal control increases the transparency of accounting information and these outcomes provide positive signal to capital market participants[7]. These studies suggest that continuous auditing system could positively affect firm value by enhancing the effectiveness of internal control and monitoring within a company. Hence, prior evidence supports the necessity of continuous auditing system.

While traditional risk management has focused on identification and management of risk at department level, ERM takes an integrated approach in risk management and changes the role & responsibilities of risk management. Within the new role & responsibilities, the department in charge of ERM is internal audit or Korean SOX department. The basic task of internal audit department is monitoring. Thus, internal auditors have monitored the effectiveness of internal control components (COSO 1) such as information & communication, control activities, risk assessment, and control environment. However, in responding to demands of external environment, internal audit function hasexpanded and become a department in charge of ERM, therefore playing a leading role in monitoringvarious ERM components (information & communication, control activities, risk response, risk assessment, event identification, objective setting, internal environment) based on COSO 2 ERM Framework.

Table 1. Comparison of COSO 1 and COSO 2 ERM Framework

Category	Year 1992 COSO/internal control	Year 2004 COSO/ERM
Achievement of objectives		Strategic
	Financial reporting	Reporting
	Compliance	Compliance
Components	Monitoring	Monitoring
	Information & communication	Information & communication
	Control activities	Control activities
	Risk assessment	Risk response
		Risk assessment
		Event identification
		Objective setting
	Control environment	Internal environment

2.2. Integrating ERM and Continuous Audit System. A continuous audit is generally defined as "a methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity's management is responsible, using a series of auditors' reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter (CICA/AICPA Committee, 1999)". As confirmed by this definition, a continuous audit requires auditors with expertise who can monitor information processed through ERP system and a continuous monitoring system as an infrastructure that can be utilized by auditors. Since a continuous monitoring system is the base for a continuous audit, it should be considered the first priority when implementing continuous audit system. In other words, an important subset of continuous auditing is the continuous monitoring of business process controls (CMBPC), a task made particularly significant by the passage of Section 404 of the Sarbanes/Oxley Act that requires both managers and auditors to verify controls over the firm's financial reporting processes (Alles Michael et al., 2006). The continuous monitoring system automatically extracts abnormal data based

[7] Doyle et al. (2007) show that weak internal audit system is related to low quality of accruals. Also, DeFranco et al. (2005) find a negative market reaction to companies who report the material weaknesses of internal audit system.

on pre-specified monitoring scenarios, which are drawn from trading data collected in every level of business under enterprise resource planning (ERP) environment.

Vasarhelyi et al. (2004) suggest that a continuous auditing is required to take advantage of advanced information technologies under an ERP environment. Computer assisted auditing techniques (CAATS) are limited, because they cannot utilize automated and integrated information technologies as done by ERP. However, ERP aims for real-time information flows in integrating and automating business processes. Therefore, when there are needs for real-time data, the potential benefits of ERP systems can be achieved only by continuous auditing. Chan and Vasarhelyi (2011) argue that the traditional audit paradigm is outdated in the real time economy and the innovation of the traditional audit process is crucial in supporting the real-time assurance. Also, they emphasize the innovation, namely the transition from traditional auditing to continuous auditing methodology.

Furthermore, research on continuous audit system that is integrated with other management systems is warranted. A continuous audit system could be utilized with connections to various management systems, for example, company A integrated audit information system and early-warning system. For ERM system, there are many cases where KRI is linked to early-warning system. Thus, continuous audit system can be integrated with ERM system by developing KRI based on continuous monitoring scenarios under continuous audit system. This will enable comprehensive risk management at process level, which is the main concern of strategic risk management and continuous audit system.

3. Case study: company A

In this section, we discuss and evaluate the case of company A (a non-financial company in Korea) which implemented ERM successfully at subsidiary level.

3.1. ERM implementation methodologies. Introducing ERM was not a one-time event. Rather, company A implemented the ERM system with comprehensive consideration of risk policies, risk management process, roles and responsibilities, supporting system and risk culture. Risk policiesare stated through ERM policies and ERM manuals. These policies determine the risk management processes, which consist of the following four stages of identification, evaluation, response and monitoring.

(1) Identify: company A identifies the risk, analyzes the risk sources, and keeps their profiles (see Table 2).
(2) Assessment: risk is assessed using guidelines and evaluation templates. The risk at priority control is managed based on the results of risk assessment.
(3) Response: company A sets the direction of risk response and implements the plans to respond and to improve risk management.
(4) Monitor/Report: KRI is monitored and the results of risk management and any improvement in risk management are reported.

Table 2. Risk profile of company A

Category	Risk
People/human resources	Risk of leaking corporate confidential information (policy, strategy, planning)
	Risk of declined business performance due to poor employee education/training
	Risk of delayed decision making due to a lack of authority designation within organization
	Risk of unfair compensation/rewards
	Risk of delayed decision making due to bad union-management relation
	Risk of inefficient workforce management because of weak ties between business plans and training plans
Financing/Capital resources	Risk of additional costs or delayed CapEx due to uneasy internal or external financing
	Risk of ineffective enterprise insurance management
	Risk of fraud/embezzlement/misstatement due to noncompliance of corporate financing policies
	Risk of reduced profits due to a lack of appointment system and its supporting system
	Risk of financial losses due to absence of asset management system

Risk management organization is composed of risk committee, risk owner, risk management department and risk officer. ERM support system and early-warning system serve as a support system. Lastly, risk culture is defined through employee education and communication, as well as the manner of managing changes.

3.2. Integration of management control system and ERM. In company A, ERM was implemented through integrating the existing management control system with risk management system. This helps to identify and evaluate the risk underlying the existing management activities. Figure 2 describes how the management system and ERM process have been integrated.

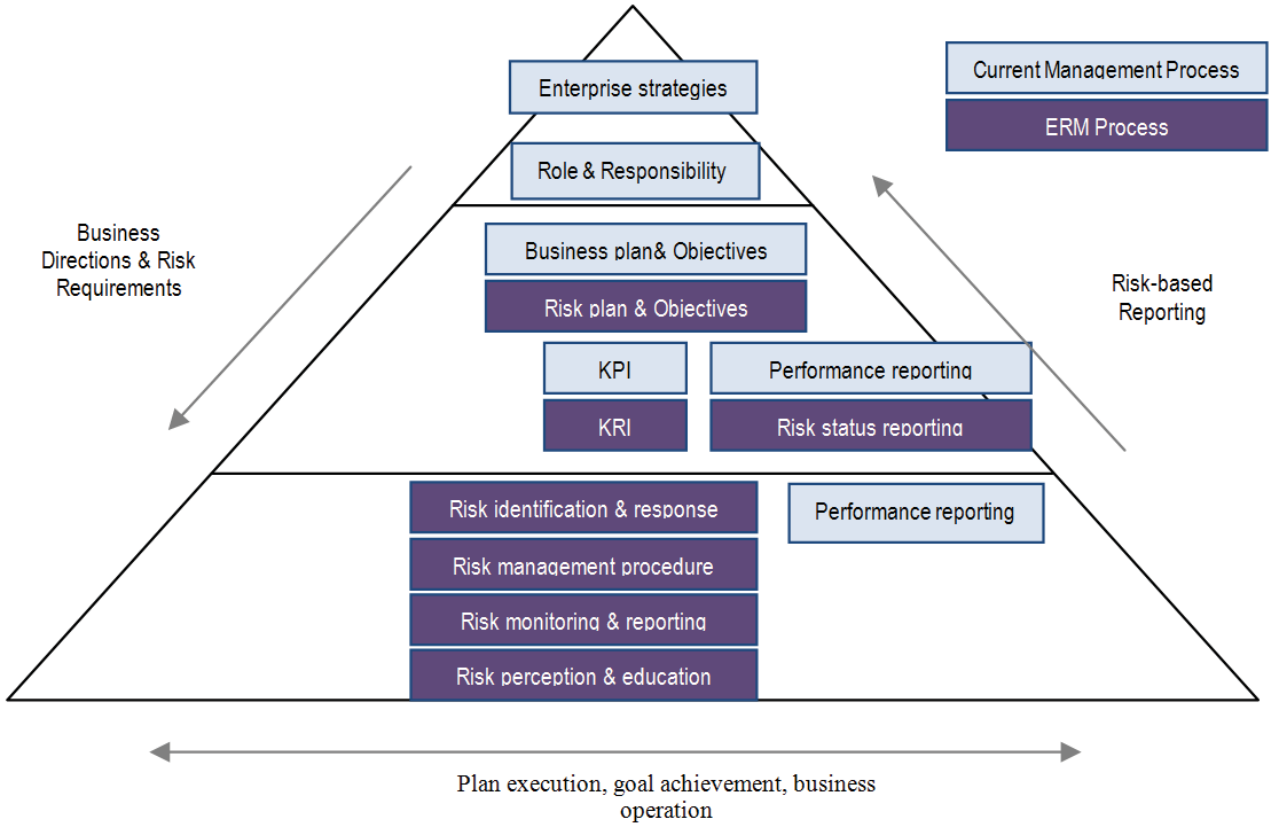

Fig. 2. Integration of ERM and management control systems

3.3. Risk management at subsidiary level. When implementing ERM, an organization should customize the process for firm-specific needs and circumstances. In case of company A, ERM implementation improved and developed risk management functions. They concentrate on the business risk, investment risk (due to global business), project risk, and financial risk. Also, the parties in charge of ERM implementation are CEO, CFO, and internal auditors. The role of CRO (Chief Risk Officer) is served by CFO.

CRO is an executive who identifies, measures, and develops the strategies to manage potential business risks. The importance of CRO has increased in recent years, since it is difficult for top executives to clearly know the level of risk, as the firm size gets bigger. Also, sustainable growth can be attained through effective response to the profile of risks, as business environment changes.

The risk governance system of subsidiaries of company A can be considered the form in the middle of centralized and delegated system (see Figure 3). It aims to build the integrated crisis & risk management system at enterprise level. ERM implementation was expanded to other subsidiaries starting from the chemical-related subsidiary. Each business unit and staff is delegated for their own risk management. A risk officer is stationed at each subsidiary in order to work on subsidiary-level risk management and support. In addition, they set up the ERM team with CRO in charge and early-warning system to prevent the major risks.

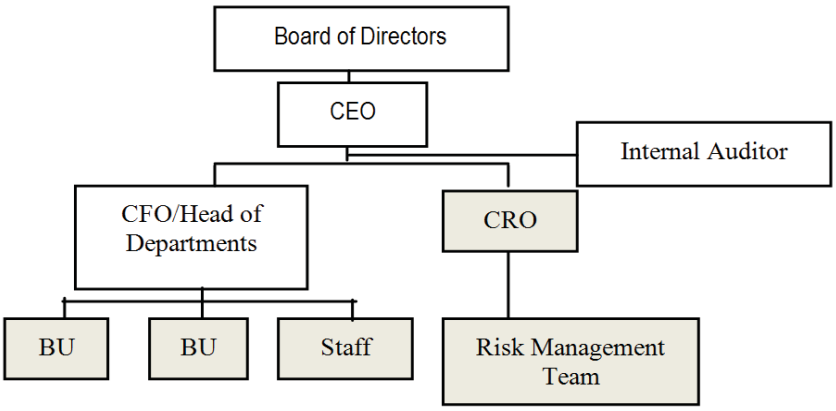

Fig. 3. Risk governance system in company

3.4. Case evaluation and discussion. ERM is a very attractive management control system for management who experienced great losses due to unexpected risk. However, ERM has not been used actively in company A, since it was implemented. The reasons for this are analyzed as follows: first, there are no practical instructions or guidelines for risk management. Second, ERM was implemented just to get along with the crowd without careful consideration of selecting KPI based on firm-specific characteristics. Third, the management's view is too myopic, focusing on short-term performance. Regarding the measurement of performance, it is not clear how to quantify the effects of KPI in preventing crises.

Then, what could be the solutions to utilize ERM more effectively? First, the management should change their perspective on ERM, from a silo-based approach to an enterprise-level management approach. This requires the consideration of enterprise-wide loss (risk) in goal (outcome)-oriented thinking. Second, they need to customize the risk-management depending on the type of major risk. For instance, Walmart (traditional, PPE-intensive company) would have to manage typical operational risk, whereas Microsoft (economy-sensitive, competitive industry) has to manage unpredictable business risk. Third, they should begin with most-necessary tasks in the field by analyzing past losses and interviewing field expertsin order to identify weaknesses. Also, KPI and KRI should be managed together. KPI should be used as a carrot-and-stick for employees while KRI is a broader concept than KPI since it navigates the enterprise goal. Risks that cannot be detected by KPI should be identified and managed through further development of KRI. Last, the leadership of risk management and (internal and external) communication should be strengthened under the direction of CEO or CRO.

Discussion and conclusions

This section discusses the measurement of maturity of ERM. As described in Table 3, a company may be assigned to level 1~5 based on the current risk management practices. There are five categories for measurement of ERM level: strategy/policy, process, organization, methodologies, and culture. Companies in level 1 have no systematic risk management system, such as risk management policy, process, clear role & responsibilities, and guidelines for methods. On the other hand, level 5 companies have established ERM culture, which attains the appropriate level of risk management. Interestingly, the reliance upon risk management team is, low as the risk management task is integrated with the routine tasks of employees.

Table 3. Measurement of ERM maturity

	No risk management system Level 1	Individual risk management system Level 2	Systematic risk management Level 3	Integrated risk management system Level 4	Established ERM culture Level 5
Strategy/policy	-No risk management strategy -Risk management decisions are made ex-post	-Strategies exist for financial risk or influential risk -Respond to previously experienced risk	-Management of various risks including financial, operational, strategic risks -Little integration with business plans	-Risk management and business plans are integrated -Risk management is integrated with performance management, investment decision making	-Enterprise-level and portfolio-level risk management -Achieves an appropriate risk level
Process	-No official risk management process	-Individual risk management processes exist, but lack consistency	-Identification and monitoring processes exist, but evaluation process is not integrated -Individual risk management	-Standardized risk management process (risk identification-evaluate-respond-monitor)	-Coordinated risk process and components of risk management (strategy, organization, methods, culture)
Organization	-No official risk management team	-Business units are responsible for their own risk management -High reliance upon external/internal auditors	-Role and responsibilities at enterprise level are defined -Risk management knowledge and skills are concentrated in specific departments	-Inidividual units are responsible for their own risk management, which contributes to continuous risk management cycle	-Less dependence on risk management team -Risk management is blended in ordinary business tasks
Methodologies	-Depends on experience and instinct -No techniques or standards	-Traditional management information system -Most risk management is based on manuals	-Limited risk monitoring and reporting system -Basic tools are used to quantify risk	-Up-to-date central database -Effective early warning system -Integrated system which can be utilized at business unit-level	-Integration among the components of risk management, integration with other business systems
Culture	-No understanding on risk management	-Most employees are aware of importance and need of risk management	-Top executives support risk management -Perception of risk management is consistent throughout the organization	-Concepts & methodologies of risk management are understood and applied at each business unit-level	-It becomes organizational culture since all members consider risk in their decision making or task execution

In conclusion, the case study of company A shows how ERM is implemented and integrated with management control in order to increase firm value by monitoring its subsidiaries. This successful ERM adoption case can be used as a guideline for other organizations, which plan to adopt ERM in the future with reduced costs and improved processes. Especially, the implication of our paper on how a group-level internal auditor uses ERM as a tool to manage risk of subsidiaries could be useful for large conglomerates, where group-level monitoring cannot control subsidiaries due to limitations of KPI and internal controls.

References

1. Alles, M., Brennan, G., Kogan, A., and Vasarhelyi, M.A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems*, *7*(2), 137-161.
2. Arena, M., Arnaboldi, M., and Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, *35*(7), 659-675.
3. Beasley, M. S., Clune, R., and Hermanson, D.R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation, *Journal of Accounting and Public Policy*, *24*(6), 521-531.
4. Casualty Actuarial Society Enterprise Risk Management Committee. (2003). Overview of enterprise risk management. *Fairfax, VA: Casualty Actuarial Society*.
5. Chan, D. Y., and Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems*, *12*(2), 152-160.
6. CICA. (1999). *Continuous auditing*. A CICA/AICPA research report.
7. COSO, S. (1992). Internal Control−Integrated Framework. *The Committee of Sponsoring Organizations of the Treadway Commission*.
8. Committee of Sponsoring Organizations of the Treadway Commission. (2004). The (COSO). (2004). *Enterprise Risk Management-Integrated Framework: Executive Summary*.
9. De Franco, G., Guan, Y., and Lu, H. (2005). The wealth change and redistribution effects of Sarbanes-Oxley internal control disclosures. *Available at SSRN 706701*.
10. Doyle, J., Ge, W. and McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting, *Journal of accounting and Economics*, *44*(1), 193-223.
11. Flesher, D. L., and Zarzeski, M. T. (2002). The roots of operational (value-for-money) auditing in English-speaking nations. *Accounting and business research*, *32*(2), 93-104.
12. Gordon, L. A., Loeb, M. P., and Tseng, C.Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, *28*(4), 301-327.
13. Meulbroek, L. K. (2002). A senior manager's guide to integrated risk management. *Journal of Applied Corporate Finance*, *14*(4), 56-70.
14. Power, M. (2009). The risk management of nothing. *Accounting, organizations and society*, *34*(6), 849-855.
15. Selim, G., and McNamee, D. (1998). Risk management: changing the internal auditor's paradigm. *Institute of Internal Auditors Research Foundation, Altamonte Springs, Fla*.
16. Vasarhelyi, M.A., Alles, M.G., and Kogan, A. (2004). Principles of analytic monitoring for continuous assurance, *Journal of emerging technologies in accounting*, 1 (1), pp. 1-21.
17. Weidenmier, M. L., and Ramamoorti, S. (2006). Research opportunities in information technology and internal auditing. *Journal of Information Systems*, *20*(1), 205-219.