An Integrated Approach to Enterprise Risk: Building a Collaborative Risk Strategy Within the Business Processes of the Enterprise

Today, most organizations continue to rely on a traditional approach to risk management. Such an approach is built on stovepipe-oriented risk management, in which the focus is mainly on the tactical business issues and does not consider strategic sources of risk. This traditional approach to risk management does not adequately identify, evaluate, and manage risk; tends to be fragmented, treating risk as disparate and compartmentalized; limits the focus to managing uncertainties around physical and financial assets; focuses largely on loss prevention, rather than adding value; tends to use linear and sequential process thinking; tends to be highly disaggregated from managing a firm's risk; and is not holistic. Moving to an enterprise risk management (ERM) program is practical, but the level of maturity in adopting ERM is different from one organization to another. Although ERM overcomes many of the limitations of traditional risk management models, it brings its own limitations and challenges.

The Business Process-centric Risk Management System (BPC-RMS) conceptual model is based on a holistic integrated approach to enterprise risk and consists of six domains and 16 processes. The BPC-RMS looks at all functional areas and describes several internal and external sources. Systems can interact with these sources to establish a repository of risk data and ensure that risk knowledge is elicited, shared and managed appropriately.

The amount of interest and research on risk management attests to its relevance. Researchers and practitioners through empirical and field studies indicate that in today’s business environment, traditional risk management practices are no longer sufficient to deal with today’s threats. Intense competition, natural disasters, financial crises, terrorism, the Internet, cyberterrorism, regulatory requirements and many other things require dealing with new levels of risk.

The inability to manage all kinds of risk in a cohesive and precise approach results in dramatic impacts on organizations to compete effectively, satisfy their customers, retain their employees, meet their financial responsibilities, and attain the goals and objectives of the organization. Moving from the traditional risk management approach to a more advanced one requires embedding risk management activities within the business processes of the enterprise and establishing a repository risk management system. The BPC-RMS system proposes a step-by-step repositioning of resources to help organizations deal in an effective and credible manner with both threats and opportunities and also bridges the gap between strategic and tactical risk management. In such a case, the entire organization is aware of the importance of risk management and it is used continuously in any process and activity rather than on an as-requested basis.

METHODOLOGY
To ensure the holistic approach rigor, the design science research process and the design science information systems research methodologies were drawn upon to develop and define the BPC-RMS:

- **Problem identification and motivation (relevance cycle)—The main problems identified are:**
  1. The current practices of risk management proved to be lacking in providing organizations sufficient framework and structure related to risk management to meet their business needs.
  2. Risk knowledge should be shared among people in different functional areas.
  3. The current traditional risk management approach is exercised in silos in organizations making it hard to create a risk culture within those organizations.
  4. The inability to manage all kinds of risk in a cohesive and precise approach results in dramatic impacts on organizations.
• Objectives of the solution (implicit in relevance)—Based on the aforementioned problems, three main objectives were identified:

1. Build a holistic business-process-centric risk management framework to help organizations meet their business needs.
2. Build a BPC-RMS based on predefined principles.
3. Help organizations integrate the risk management function into the business processes of the enterprise in order to compete effectively, satisfy their customers, retain their employees, meet their financial responsibilities, and attain their goals and objectives.

• Design and development (iterative search process)—To explicate the design of the solution that fulfills the objectives, an extensive review of related literature was carried out; it proposed that no sufficient risk management conceptual framework solution existed. Hence, advancing the view of risk management by moving it from a stovepipe approach to a holistic approach is proposed in this article, through several iterations to ensure a complete and sound solution. To address the first objective noted above, the building blocks of the holistic framework were identified in light of BPC-RMS. To address the second objective, the BPC-RMS model was introduced with a predefined set of principles and the model was extended by introducing a set of elements to address requirements that come from service-oriented architecture (SOA) service standardization efforts and are enabled based on the business process requirements. To address the third objective, the validity, usability, adaptability and usefulness of the framework were studied, comparing it with the current ERM software packages that organizations adopt or develop in-house. Thus, the BPC-RMS solution was positioned accordingly.

• Evaluation (evaluate)—Preliminary evaluation regarding the validity, usability, adaptability and usefulness of the proposed framework was completed. The model was evaluated in terms of its objectives. Then, the adoption levels of the ERM within organizations were evaluated, and the technology of software packages that organizations adopt or develop in-house was identified and evaluated. During the process, the most popular risk management solution packages were identified, the functional emphasis and the market focus for these packages highlighted, and the solution in relation to these characteristics positioned.

RISK MANAGEMENT COMPONENTS, FRAMEWORKS, MODELS AND TECHNIQUES

The BPC-RMS solution was developed after thorough evaluation of current literature related to risk, risk analysis and risk management from several organizations and researchers. For example, the COSO 2004 framework provides a detailed description of the essential components and clear direction and guidance for ERM. Critics of the COSO 2004 framework claim that the framework is a broad, principle-based document not particularly suited for internal controls monitoring. The traditional audiences for COSO have been internal and external auditors and members of the accounting community; thus, some say that COSO is too complicated to be applied and used by midlevel managers and business units and takes the approach of command and control while ignoring shared management of uncertainties and social implications of ERM. The newly released COSO 2013 Internal Control—Integrated Framework is an updated version of COSO’s 1992 framework and is considered to be complementary to COSO’s 2004 ERM framework.

COBIT 5 covers risk management in the governance and management of enterprise IT (GEIT) areas. COBIT 5’s EDM03 (Ensure risk optimization) process is one of five processes of the Evaluate, Direct and Monitor (EDM) domain of the governance area. EDM03 focuses on stakeholder risk-related objectives to ensure that the enterprise’s risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed. In addition, EDM03 ensures that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is
identified and managed, and the potential for compliance failures is minimized. The APO12 (Manage risk) process is one of 13 processes of the Align, Plan and Organize (APO) domain of the management area. APO12 continually identifies, assesses and reduces IT-related risk within levels of tolerance set by enterprise executive management. Also, APO12 integrates the management of IT-related enterprise risk with overall ERM, and balances the costs and benefits of managing IT-related enterprise risk. Moreover, all enterprise activities have associated risk exposures to ensure that the enterprise stakeholders’ approach to risk is articulated to direct how risk facing the enterprise will be treated. ISO/IEC 15504 is the reference for the maturity models and its Software Process Improvement and Capability Determination (SPICE) is a set of technical standards documents for the computer software development process and related business management functions. COBIT 5 assessments for process capability are designed and built to follow ISO/IEC 15504.

New South Wales classifies risk in the following categories: strategic, compliance, financial, operational, and market or environmental. The Orange Book classifies external risk (arising from the external environment) categories in the Political, Economic, Sociological, Technological, Legal and Environmental (PESTLE) model. The COSO ERM framework defines the context of entity objectives into four categories: strategic (high-level goals aligned with and supporting the mission), operations (effective and efficient use of resources), reporting (reliability of reporting) and compliance (compliance with applicable laws and regulations). Combinations of these categories are used in the BPC-RMS components.

The lack of solutions for an advanced risk management practice and the potential value organizations can gain from adopting such solutions are important and relevant to the study of risk management. Relevance as one main cycle of the design science methodology is well defined in the BPC-RMS framework. Demonstrating the important role risk management plays in business and strategic planning and providing a comprehensive framework to run such a practice in an effective and efficient manner will help organizations integrate risk into their business processes. And, as a result, organizations can utilize their resources effectively, minimize surprises and shocks, enhance communications between internal and external entities, and move ahead of competitors when it comes to grasping opportunities.

Beyond Traditional ERM

Today, several companies have undertaken risk management initiatives to assess their risk management maturity and, as a result, aggregated and developed risk management profiles and risk appetites aligned with the company’s strategic objectives. Such initiatives are still in development and are based on best practices to help organizations in producing a number of cost benefits.

Although COSO ERM overcomes many of the limitations of the traditional risk management models, it brings its own limitations and challenges. One of the biggest problems of deploying ERM is limiting internal audit’s scope to one of the three key objectives of the framework.

The limitations section of COSO ERM’s executive summary points out that no matter how well planned, designed and implemented, ERM can provide only reasonable assurance to the board of directors and management that the entity’s objectives will be achieved. Such limitations result from several factors such as COSO’s audit roots, judgment in decision making, management overriding ERM decisions, inaccurate calculations, incomplete information and the breakdown of internal controls. The BPC-RMS framework overcomes many of these limitations through its three components, as described in the following sections.

The Business Process-Centric Risk Management System

In a 2005 survey, the integration of risk systems in business processes ranked as a top obstacle to success. The study concluded that, “This reflects the difficulty firms face in capturing data on risk events, and on integrating those data from a multitude of systems to build a clear and accurate view of risks across the business.” In a quickly evolving, competitive business environment, it is essential that firms develop an integrated risk management system to capture data on risk events and be able to analyze the effect of one risk event on another across functional areas.

After the analysis detailed in the previous sections, a multiphase iterative abstraction exercise was carried out, in which the proposed components of the BPC-RMS were reviewed and identified. As such, some components of already-established frameworks were used. For example, the COSO ERM framework provides a detailed description of the essential components of risk management and clear direction and guidance for ERM. COSO ERM describes several internal and external sources of data that are useful in affecting
ERM. The external resources that have been adopted for the framework are customers, vendors, business partners, external auditors, regulators and financial analysts. These resources are among the external entities that are affecting the quality of data that the system is acquiring. The BPC-RMS utilizes these resources as shown in figure 1. By acquiring such data, the system establishes a repository of risk data and ensures that information and risk knowledge are elicited, shared and managed appropriately.

The internal resources in the BPC-RMS framework include business owners, senior management, the risk management department, the financial and accounting department, the purchasing department, the internal audit department, the sales and marketing department, the human resources department, the production department, the IT department, the security department, and the CEO and board of directors. These resources are trusted to provide input and utilize the system to assess and control risk associated with the respective job functions.

The proposed BPC-RMS gives organizations more control in fulfilling compliance requirements from their own policies, as well as government legislation. The design science methodology called for several iterations before arriving at the proposed solution. After the literature review, the initial hypotheses and principles that guided the early design of the BPC-RMS were identified. Next, an iterative process of designing, collecting evidence, and evaluating the design in terms of meeting the aforementioned objectives was undertaken. These insights were
then used to redesign the conceptual framework to improve the effectiveness and the efficiency of the system.

The BPC-RMS consists of six domains—plan and prepare; assess; share; integrate; mitigate; and monitor, control and evaluate—and 16 processes (risk services).

The plan and prepare domain is responsible for and covers determining risk resources and categories, defining risk parameters, and establishing risk strategy.40 The assess domain is responsible for and covers assessing the risk by identifying, analyzing, categorizing and prioritizing risk. The share domain is responsible for and covers controlling the participation and the collaboration among stakeholders. The integrate domain is responsible for managing the cross-functional risk in the system and covers revising and integration. The mitigate domain is responsible for providing the framework to deal with strategic actions to mitigate risk and covers developing risk mitigation plans and implementation. Finally, the monitor, control and evaluate domain is responsible for providing mechanisms to monitor, control, evaluate and report risk status. The domains interact with each other through a common risk management repository.

The share and integrate domains are very important for progressing discussions among internal and external stakeholders. In such a setting, participation and collaboration among potential participants in the share domain enforces the practice of improving discussions and collaborations among these players and helps to interchange risk information in an effective and efficient way. For example, department managers, chief financial officers, chief administration/operations officers, chief technology officers, legal/audit staff, information security and others participate and coordinate among themselves after identifying risk factors in their areas by examining the impact of risk identified in other areas and/or if one risk factor positively correlated with another risk factor. Furthermore, the outcome of such a dialog can help in the integration and the revision of risk.

The risk services should be integrated with the six domains of the BPC-RMS. By focusing on the business processes, the organization determines during the initiation phase of the system development which risk services within each domain will be required to be part of the system. The data flow diagram in figure 2 describes the BPC-RMS domains and the processes (risk services) associated with each domain.

The data should be maintained in the risk management repository and all activities interacting with the data should maintain the security, compliance and operational business data requirements.41 The stakeholders of the system expect the security requirement to maintain appropriate levels of confidentiality, integrity and availability. They expect compliance requirements to maintain appropriate levels of compliance and reliability, and they expect the operational requirements to fulfill effectiveness and efficiency requirements.

As part of the BPC-RMS, organizations need to build trust, control, and independence and share models (figure 3). The building of trust is an important social process that is widely accepted as a prerequisite to knowledge sharing and cooperation.42-45 Research has shown that knowledge sharing relies on trust in the receipt of useful knowledge46 and the levels of trust influence the exchange of resources between intraorganizational business units.47 Competence, integrity and benevolence are positively related to knowledge-sharing behavior.48 These dimensions (processes) must be integrated within the BPC-RMS to permit the sharing of risk knowledge.

Trust allows internal and external entities to interact with the BPC-RMS within the boundaries of control that the system can provide. The system must have enough control built on the concept of being compliant with internal policies and procedures and legislation requirements. Sharing and independence are important in certain business settings. For example, auditors, as per their job description, must maintain their independence and, at the same time, share their knowledge and expertise with the rest of the organization’s entities.

ADOPTION LEVELS OF THE ERM PACKAGES

Although ERM has been discussed at length by practitioners and researchers, it is still a “rather elusive and under-specified concept” and “little progress seems to have been made in achieving this elusive nirvana.”49 Little is known about the stages of COSO ERM deployment or factors that affect the embrace of ERM within organizations.50, 51 Considering different factors to assess COSO ERM adoption levels within organizations, the presence of a chief risk officer, board independence, CEO and CFO apparent support for ERM, a Big Four auditor (i.e., KPMG, Deloitte & Touche, Ernst & Young, PricewaterhouseCoopers), entity size, and entities in the banking, education and insurance industries are positively related to the adoption of ERM. Introducing key risk indicators

©2014 ISACA. All rights reserved. www.isaca.org
(KRIs), identifying the potential benefits of developing a set of KRIs, and emphasizing the importance of establishing an appropriate methodology for communicating KRI data to members of the board and senior management are critical.\textsuperscript{52}

Organizations can develop ERM solutions in-house or adopt ERM solutions through consulting firms or from software vendors. Line managers are involved in the development and administration aspects of risk management and they should be involved in the selection and the usage of the commercially available ERM software packages. Although ERM technology is evolving at a rapid pace, solutions developed internally become quickly outdated, require change, and are often geared toward compliance and audit.

Several organizations have published studies about ERM platform vendors—covering specific criteria, the weighing of each criterion and the vendors’ scores based on weighing criteria.\textsuperscript{53-56} Reviewing the 2009 Risk and Insurance Management (RIMS) study, which covers the functional emphasis and the market focus for top ERM solutions providers, the survey respondents were evenly split between companies above and below US $1 billion in annual revenues; ERM process implementation is more ubiquitous
among larger companies. In the same survey, 47 percent of the responding organizations reported using software to support the ERM process. Forty-eight percent of organizations reported that they do not use software to support ERM processes, 27 percent were developing their own solutions internally (using desktop applications), 5 percent were developing custom solutions and 20 percent reported using specialized software. In short, there are as many variations of ERM, at a detailed level, as there are organizations practicing ERM. These variations occur since no single ERM solution fits all of an organization’s needs. Customization of ERM software is necessary since the business models and business processes are different from one organization to another.

Responses from companies who participated in the RIMS survey emphasized the importance of compiling data, analysis, reporting, monitoring and tracking capabilities in the selection of ERM software packages. These results did not change when the participants were asked how they would like to use ERM technology in the future.

The six domains and 16 risk services of the BPC-RMS enforce the practice of improving discussions and collaboration among the internal and external stakeholders and help in interchanging risk knowledge effectively and efficiently. As such, and reflecting on the functional emphasis as described previously, the BPC-RMS framework can be used effectively for data management, reporting, systems integration, monitoring and tracking, and can be easily integrated into the established financial analysis system that an organization is using. Compiling risk data and reporting capabilities are provided through the data management capabilities of the BPC-RMS system. In addition, the BPC-RMS integration with other systems within the
organization (such as enterprise resource planning [ERP]) provides a rich database system that can be used within the structure of the BPC-RMS to provide background information about the company business.

IMPACT ON PRACTICE AND FURTHER AREAS OF RESEARCH
The proposed BPC-RMS solution helps in overcoming the challenges and limitations that practitioners have had in applying the traditional or ERM approaches. As per the analysis discussed earlier, it is clear that the current practices of risk management do not provide a level of confidence to decision makers that such approaches will help in meeting their business goals. In addition, organizations are missing a huge opportunity to capitalize on best practices when it comes to risk management. The proposed BPC-RMS framework and solutions are designed to increase the confidence of management regarding the way functional teams are cooperating when it comes to dealing with risk and help increase the probabilities of analyzing risk in a dialog setting. In turn, by creating risk knowledge, the framework and associated solutions increase the success factors of mitigating and responding to all levels of risk.

The proposed framework has not been implemented in real-world applications. It is a conceptual framework based on a design science approach. It does not include empirical validation. Future research should endeavor to validate the framework developed in this study. Another area for research is to develop business process controls as one of the potential ways to respond to risk that has been evaluated for the BPC-RMS. Such controls will provide assurance about the quality of the data collection process and the accuracy process. In addition, the controls will provide assurance about the interactions of internal and external entities and the flow of data and information among the domains’ components of the BPC-RMS. Control systems enable management to meet this responsibility.

Further work should attempt to show how methods of integrating risk into the business processes used in this study are appropriate across all business processes.

CONCLUSION
The development of an ERM framework is an ongoing effort by many organizations, and it has an influential role in shaping organizationwide risk strategies and policies in a shared governance structure. This article addresses a number of issues related to the current implementations and adoptions of ERM. By using the sciences of design methodology, an integration of risk data into the business process of the enterprise is proposed. Though conceptual developments in this article are limited to requirements analysis and high-level design, they could easily be extended to cover system design and implementation.

Risk management must be fully integrated with the business processes of the enterprise. Thus, a holistic approach that is consistent with the BPC-RMS is proposed. In the traditional approaches to risk management, risk is ranked and prioritized as part of risk handling based on the likelihood and the business impact of each risk; for example, stopping the improper release of patients’ medical information may take precedence over a virus that defaces a web page on an internal test server.

REFERENCES
DACS Gold Practice, Document Series GP 12 V 1.0, Formal Risk Management, 2004

ENDNOTES
3 Ibid.

Ibid.


Papadaki, K.; D. Poleni; “Collaboration and Knowledge Sharing Platform for Supporting Risk Management Network of Practice,” The Third International Conference on Internet and Web Application and Services, Institute of Electrical and Electronics Engineers (IEEE), 2008

Op cit, Woodhouse, 2008


CMMI IPPD Project Management (CMMI), www.niwotridge.com/PMasSE/CMMI_IPPD/CMMI.html


Murthi, S.; *Preventive Risk Management for Software Projects*, Institute of Electrical and Electronics Engineers (IEEE), 2002


Ibid.


Ibid.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, Executive Summary, May 2013

Op cit, NSW

Op cit, HM Treasury


Ibid.

Op cit, Shaw, 2006

Op cit, Williamson, 2007

Op cit, Shaw, 2006


Op cit, Hevner, 2004