"An Integrated Approach to Enterprise Risk: Building a Multidimensional Risk Management Strategy for the Enterprise"

Munir Majdalawieh, John Gammack
{Munir.majdalawieh, John.gammack}@zu.ac.ae

ABSTRACT

The development of enterprise risk management frameworks is an ongoing effort by various organizations and has an influential role in shaping organizational-wide risk strategies and policies in a shared governance structure. Investigating the perceived silo-based nature of risk management and the relevant risk function integration and communication holistically however, remains a challenge. The main objective of this study is to address this significant problem by proposing a multidimensional Risk Management framework with three key domains: a Business Process-Centric Risk Management System (BPC-RMS), a Risk Dialogue Matrix (RDM) based on Expert rules and Data-Mining, and a Risk Management Program (RMP) led by a Risk Management Office. A holistic multidimensional risk management approach looks at all functional areas in the enterprise, identifies all the risks in these areas, analyzes their relationship and impact, and provides a balance among all risk activities. The proposed framework is designed to build upon the standards and best practices of risk management. Using design science methodology, we propose and evaluate a multidimensional framework to integrate these risk management concepts into the business process of the enterprise.

Keyword: Risk, Risk Management, Risk Assessment, Risk Control, Risk Response, BPC-RMS, RMP, RMO, RDM, SOFIC model, Enterprise Business Processes, Risk Integration, Risk Communication

INTRODUCTION

Risk management is designed to identify potential events that may affect the organization[1], manage risks to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives (COSO, 2004).Risk management, among other things, requires embedding of risk management responsibilities into the organization, and understanding of compliance requirements (ITGI, 2007). Focusing on "***risk culture***" and "***strategic risk management***", Standard & Poor has factored enterprise risk management(ERM) activities into its overall rating of management and company outlook since 2008, giving companies extra incentive to think seriously about implementing ERM in their organizations (Aon, 2009).

The amount of interest and research on risk management testifies 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 emerging threats (Woodhouse, 2008; PWC, 2015).

[1]Throughout this paper, we will be using "organization" as a generic reference to large or small businesses, government, or not-for-profit entities.

Intense competition, natural disasters, financial crises, terrorism and cyber terrorism, along with regulatory requirements and many others require dealing with new levels of risk, exacerbated by the speed of onset fostered by Internet and a 24/7 news cycle(Layton & Wagner, 2007).

Since risk in one functional area could very much affect a risk in another area, such "risk knowledge" could help in defining more precise and cohesive strategies about how to deal with risk. As such, "risk knowledge" should be shared among people in different functional areas (Papadaki& Despina, 2008; Rodriguez and Edwards, 2014). In such environments, people should be able to share risk knowledge in an ad-hoc setting, rather than coordinating with others who are in the same field with similar expertise. Moving to such a level of "risk knowledge" and establishing "risk culture" requires the establishment of a *risk management program* (RMP) led by a risk management office (RMO) to ensure that risk management knowledge will be shared among people in different functional areas and to integrate all risk-related activities into a single, comprehensive model that better analyses and minimizes risk to an organization. After the 2008 financial crises, risk management has been an important agenda item of the business enterprises since it leads to better decisions and enhances performance (Gates et al. 2012). Farrell and Gallagher (2014) concluded that firms show a 25% gain in performance value when the level of top–down executive engagement and the resultant cascade of ERM culture throughout the firm.

In this study we aim to contribute both theory and management practices related to risk management, and to add to the ongoing debate about whether the current practices of risk management are sufficient to help organizations meet their objectives and goals. Current practices of risk management are lacking in providing organizations with sufficient framework and structure to meet business needs. In particular, "lack of integration and communication appears to be one of the most significant problems" and companies with segregated risk management fared worse in the 2008 crisis (Harner, 2010:1335).A structural focus on separate business units does not necessarily effectively address enterprise wide risks, despite COSO's provision for entity level consideration. A major criticism of COSO (Marks, 2011) is that it confuses the framework (organizational structures and policies) with the process of risk management (the integration of assessment and monitoring into processes where decisions are made).Other researchers, (e.g. Lundquist, 2014), found that different components of ERM proposed by COSO framework are used in measuring ERM quality and effectiveness, and that these have been proven as influential in improving corporate performance. In this paper we propose an integrated, multidimensional approach to enterprise risk, in which we are recommending a business process-centric risk management system to integrate all processes of risk management and interactively engage all responsible parties in such a system. Such integration would be managed and controlled through a risk management office. Moreover, a new Risk Dialog Matrix is proposed to enhance the shared risk knowledge concept to integrate risk among different business units or functional areas.

In the following sections, we examine the literature and discuss the traditional risk management approach. We then describe our methodology and develop our framework starting from the business process centric risk management approach followed by a discussion of the risk dialogue matrix, and the integrated program coordinated by the risk management office. This is followed by an initial evaluation by professionals and a discussion of the implementation of enterprise risk management. Finally, the impact on practice and conclusion of the study are presented together with ideas for future research.

BACKGROUND

RISK MANAGEMENT COMPONENTS, FRAMEWORKS, MODELS, AND TECHNIQUES

Many researchers and organizations (McShane et al. 2011; Baxter et al. 2013; Mikes & Kaplan 2014; Lundqvist 2014; Pagach&Warr 2010; CGMA 2015; COSO 2004; Orange Book 2004; ITGI 2007; ITS 2007;Stoneburneret al. 2002; Holmes 2002;Alexander & Sheedy 2005;ISO 31000:2009) have written about the topic of risk, risk analysis, and risk management by proposing methodologies, frameworks, techniques, tools, and empirical studies. For example, ISO (2009) defines risk as "the effect of uncertainty on objectives". In general, risk is the potential exposure to damage of an activity or an asset. Moreover, risk has to be connected with enterprise activities to help organizations meet their goals and objectives: ISO (2009) defines risk management as "coordinated activities to direct and control an organization with regard to risk", while Stoneburneret al. (2002) define risk management more operationally as: "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Del Bel Belluz (2012) further highlights organizational culture in her definition: "The culture, processes and structures that are directed towards the realization of potential opportunities and the effective management of adverse effects". In general, risk management concerns the processes established at an organization that help managers assess risk, determine the acceptable level of risk and then adopt strategies to control the risk. The assessment of risks includes identification, analysis, and prioritization. To a large extent however this is done only within silos, and there is a widely held view of "a distinct lack of information on how to bring all the silos together" for which COSO was found complex and "(not) the most useful for actual practice" with roughly half of firms surveyed seldom using its recommendations (Fraser and Simkins 2009).

Today many organizations still rely on stovepipe oriented risk management tools in dealing with risk. Our proposed solution is to advance the conceptualization of risk management by moving it from a stovepipe approach to a multidimensional holistic approach. A holistic approach looks at all functional areas, identifies all the risks in these areas, analyzes their relationship and impact, and provides a balance among all risk activities. A business process focus allows alignment of cross functional activities with strategy and its achievement. We operationalize our viewpoint by introducing three dimensions to the holistic approach: business process-centric risk management system, risk dialog matrix, and a risk management program coordinated by the risk management office. These three dimensions need to be part of the enterprise risk management solution to bring about the multidimensional holistic approach.

To develop our solution, we examined many articles and research papers from organizations and researchers. For example, COSO (2004) provides a detailed description of the essential components, and seeks to provide direction and guidance for enterprise risk management. Critics (e.g. Shaw, 2006) of the COSO framework however claim that the frame work, as a broad, principle-based document is not particularly suited to internal-controls monitoring. The traditional audience for COSO has been internal and external auditors and members of the accounting community, with a compliance, rather than strategic, focus. This is why some are saying that COSO is too complicated to be applied practically and for use by midlevel managers and business units (Shaw, 2006; Williamson, 2007). Furthermore, Williamson (2007) argues that COSO takes a command and control approach and ignores shared management of uncertainties and social implications of ERM.

A second theme that emerged from our review concerns the sharing of knowledge across functional units. Knowledge management practices and shared repositories of information can support decisions here, and Rodriguez and Edwards (2009) report work showing an association between the perceived value of ERM implementation and the quality of knowledge sharing about risk. Apart from the technological support for knowledge sharing a supportive organizational culture is critical for implementing risk management effectively. Del Bel Belluz(2010) describes two otherwise comparable companies but which differed in organizational culture (including risk mindset), employee and partner relationships, business processes (one could sustain innovation) and results (consistent profitability or otherwise), highlighting the importance of organizational context in effective ERM, and she particularly commends ISO31000 in this regard. These aspects are well researched in knowledge management (KM), whose core processes, including capturing and sharing knowledge, are related to risk management by Rodriguez and Edwards (2009).Massingham (2010) describes the emerging field of Knowledge Risk Management (KRM) and the case study he describes suggests the value of including knowledge management constructs over traditional approaches to risk management. Similar approaches integrating KM with ERM, both theoretical and practical, are reported by Alhawari et al. (2012) with sector specific integrations in e.g. software engineering/ IT projects (Ardimento et al. (2011)), telecommunications (Taletet al., (2014)), and construction (Arrow, 2008). These studies point to the centrality of knowledge in assessing risks and its embeddedness throughout the organization.

While local knowledge of unit managers is certainly relevant to identification and assessment, general settings around risk appetite and strategy are more appropriately centralized (Economist Intelligence Unit, 2007). Layton and Wagner (2007) call the compartmentalization of risk by departments the “silo factor” whose effect is to prevent top managers understanding enterprise wide risk, and which brings numerous other associated problems (CFO, 2014). These include duplication, gaps, lack of relevant communication, varying risk philosophies, and the potential for a risk in one area to rapidly propagate to affect others. These problems make it difficult to create an enterprise wide risk culture. This entails a shared overarching framework, but should also pervade everyday decision making processes.

A portfolio view that allows consideration of the interrelationship among risks is essential, and this “net assessment” can be properly referenced to a centralized strategy and risk appetite. To illustrate, in Gammack (1991) a set of modular expert systems was developed to identify risk in UK life insurance and personal loan applications. These modules separately addressed quantified, business rule-based risks associated with lifestyle, medical, travel, financial and other categories in the application form. The interactions among these areas was a non-trivial challenge as risks could compound one another or, conversely, mitigate each other. A doctor (safe) in Australia (safe) might have to fly a small plane to remote bush land (unsafe), or a skilled but unemployed worker (financially risky) intending to take employment in the Middle East (risky) might suddenly become financially low risk. Simply combining the numbers failed to give a realistic picture, motivating a more holistic design involving contextual judgment: similar stove piped and model-heavy risk management, (together with an overly aggressive risk culture) led to the downfall of RBS (CFO, 2014).A frequently expressed recommendation by holistic approach advocates is by all means to consider the numbers, but to exercise judgment as well.

Although many ERM frameworks and proposals exist, these are often sector specific, or pitched only at a general level of guidance. CGMA (2015) found that about 60 percent of 1,300 executives in organizations worldwide agree that they face a wide array of complex and increasing risk issues, despite that 35 percent or fewer organizations claim to have formal ERM in place. Lundqvist (2014) indicates that there exists no real consensus about the value creation and inconclusive of the implementation of ERM because of the multiple frameworks for the implementation of ERM. McShane et al. (2011) specifies that although ERM has emerged as a framework that supposedly overcomes limitations of silo-based traditional risk management, yet little is known about its effectiveness on the firm's performance. Consulting firms also offer frameworks and because of the unique context of each enterprise it is normal that one size does not fit all, so proprietary solutions are likely torequire non-transferrable customizations. Whilst dominant frameworks unsurprisingly outline similar areas around identification, assessment and monitoring, philosophical differences exist, with implications for implementation. COSO's structural and compliance emphasis is weak on process and context, whereas McKinsey's framework sees ERM not as a function, but as the consequence of successfully interacting processes, emphasizing culture and behavior in the comprehensive inaction of five core capabilities. Their process view moves ERM towards a more strategic role from a focus on compliance, but where the procedures involved are "articulated(in various) institutional languages" (McKinsey, 2013). Respondents in Fraser andSimkins (2009) study reported "a distinct lack of information on how to bring all the silos together—otherthan to say that a common reporting system and language are important", and this is a feature of the ISO31000 standard, which established a common risk vocabulary, but does not provide a specific framework.

METHODOLOGY

The lack of solutions and implementations for an advanced risk management practice and the potential value organizations could gain from adopting such solutions are clearly relevant in the study of risk management. Relevance is one main cycle of the design science methodology and is well defined in our framework. Not only it is important to identify the role risk management must play in business and strategic planning but also to provide a comprehensive framework to apply such a practice in an effective andefficient manner. Efficiency involves helping organizations integrate risk into their business processes and as a result, organizations will utilize resources effectively, minimize surprises and shocks, enhance communications between internal entities and internal and external entities, and be ahead of competitors when it comes to grasping opportunities, the upside of risk often neglected in a focus on control and threat avoidance.

To ensure rig our in solution development, we draw upon *the design science research process* (Peffers et al., 2008) and the design science information systems research methodology (Hevneret al., 2004). This involves a design cycle where arte facts are designed and evaluated. This approach is appropriate in the development of theoretical arte facts such as models, frameworks and other constructs, and we now define its guiding steps in the context of this study:

- *Problem identification and motivation* (relevance cycle)

The background section above reviewed the literature to understand the problems that motivate the need for and drive the development of the multidimensional business Process-Centric Risk Management framework. Summarizing, the three main problems identified are (a)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 (Harner, 2010); (b) risk knowledge should be shared among people in different functional areas (Papadaki& Despina, 2008); (c) The current traditional risk management approach is exercised in silos in organizations (Woodhouse, 2008): in such environments it is hard to create a "risk culture" within organizations; and (d) The inability to manage all kinds of risks in a cohesive and precise approach results in dramatic impacts on organizations.

- *Objectives of the solution* (Implicit in "relevance")

Based on the aforementioned problems, we identify five main objectives of this study: *(obj1)*to build a multidimensional business process-centric risk management framework to help enterprises meet their organization's needs; *(obj2)* build a Business Process-Centric Risk Management System (BPC-RMS) based on predefined principles;*(obj3)*establish a risk management practice for planning, designing, implementing, and maintaining to help organizations create a "risk culture" and share the risk knowledge among people in multifunctional areas; *(obj4)* build a risk dialog score formula to analyze and balance among all risk activities to help organizations to manage all kinds of risk; and *(obj5)*help organizations integrate the risk management function into their business processes of the enterprise to compete effectively, to satisfy their customers, to retain their employees, to meet their financial responsibilities, and to meet their goals and objectives.

- *Design and development* (Iterative search Process)

To explicate the design of the solution that fulfills these objectives, we first carried out an extensive review of related literature (summarized in the previous section), which indicated that currently no sufficient risk management conceptual framework solution exists. Hence, advancing the view of risk management by moving it from a silo approach to an enterprise approach to a multidimensional approach is proposed in this paper through several *iterations* to ensure that we have a complete and sound solution. To address *(obj1)* we identified the building blocks of the multidimensional framework in light of three key domains: 1) *Business Process-Centric Risk Management System (BPC-RMS),* 2) *Risk Dialog Matrix (RDM),* and 3) *Risk Management Program(RMP).* To address *(obj2)* we introduced the BPC-RMSmodel with a predefined set of principles, then we extended the model for generality across implementations. This was done by introducing a set of elements to address requirements that come from Service-Oriented Architecture (SOA) service standardization efforts to be enabled based on the business process requirements. To address*(obj3)* we outlined a risk Management Program for planning, designing, implementing, and maintaining to help organizations create a "risk culture" and share the risk knowledge among people in multifunctional areas. To address *(obj4)*we built a risk dialog score formula to analyze and balance among risk activities to help organizations to manage all kinds of risks. To address *(obj5)*we studied the validity, usability, adaptability and the usefulness framework by comparing it with the current ERM software packages that organizations adopt or develop in-house prior to a representative stakeholder evaluation.

- *Evaluation* (Evaluate)

Preliminary evaluation regarding the validity, usability, adaptability and usefulness of the proposed framework are discussed in a later section. We evaluate the model in terms of the objectives of our study and how our proposal is viewed by risk professionals across the general areas and how an office leading a risk program would cover. In order to assess the necessary insight in the practicality of our framework, we developed and administered a survey to risk management practitioners who are members of the ISACA organization in the United Arab Emirates in addition to many executives in the public sector.

MULTIDIMENSIONALRISK MANAGEMENT FRAMEWORK

In the following sections we will explain the three domains of the proposed multidimensional framework as shown in Figure 1.

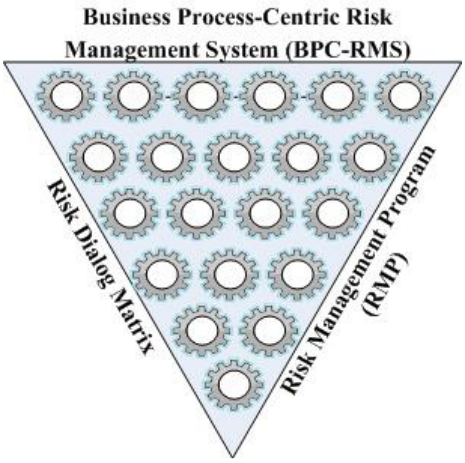

Figure 1: Multidimensional Holistic Approach

THE BUSINESS PROCESS-CENTRIC RISK MANAGEMENT SYSTEM (BPC-RMS)

Majdalawieh (2014) proposed the structure of the Business Process-Centric Risk Management Systems (BPC-RMS) in which organizations need to build trust, control, independence, and share models. The BPC-RMS represents one of our three domains of our multidimensional risk management framework covering 16 risk service areas (figure 2).

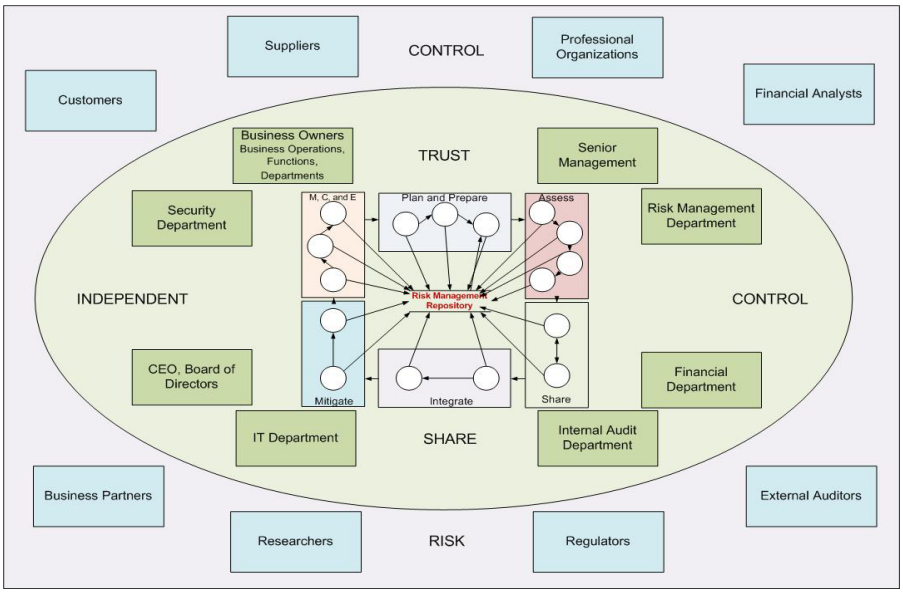

Figure 2: The interaction of the BPC-RMS System with internal and external entities (Majdalawieh 2014)

The BPC-RMS fulfills the compliance requirements from the companies own policies and the government's legislations.

THE RISK DIALOG MATRIX

Markowitz (1952) introduced the Modern Portfolio Theory (MPT), where, in order to determine the impact of relevant (systematic) risk of any individual financial asset to the riskiness of well diversified financial portfolio, correlations between all pairs of assets should be calculated. There are numerous critics of MPT. Mangram (2013) summarized some of the key criticisms as: Investor 'Irrationality' (Morien, n.d.); Higher Risk = Higher Returns (McClure, 2010); Perfect Information (Bofah, n.d.), Unlimited Access to Capital (Morien, n.d.); Efficient Markets (Morien, n.d.); Investment Independence (McClure, 2010); and there is no such thing as a "truly risk-free" asset (McClure, 2010).

In this study, we developed a simple and a new risk dialog score formula that has been borrowed from the concept of Markowitz's MPT to reflect on the need for the new BPC-RMS system as a shared repository between all stakeholders. All enterprise (dialog) risks can be calculated by this formula. In this formula, a risk dialog is calculated according to the combination of the function of impact and likelihood of a risk plus the function of impact and likelihood of other risks on the calculated risk, and a corporate risk appetite factor. The first step in using the formula is by creating the standard Risk Probability Impact (PI) Matrix. This matrix will be developed using the combination of probability (likelihood) and impact identified by each functional area, department, or project manager. The risk dialog matrix is built on the PI Matrix which is used in the traditional risk management model by analyzing risk using the following standard formula:

$$\mathbf{Risk_i = (P_i) \times (I_i)}$$

Where:

(P_i) is the Probability (likelihood)of occurrence of eventi, and
(I_i) is the Impact of eventi

Traditionally, the probabilities (likelihoods) and the impact factors are determined by the risk manager within a functional area.

The second step in using the formula is by creating a risk dialog matrix similar to the one shown in Table 1. The risk dialog matrix will help different parties to identify and quantify the impact of one risk in one department on another risk in another department or a function area. The rows and columns of the risk dialog matrix represent all the risks identified from all function areas driven from step 1.

The elements of the risk dialog matrix are donated by $I_{j,i} \times P_j$where $I_{j,i}$ is the calculated impact of $risk_j$ on $risk_i$, and P_j isthe calculated likelihood of $risk_j$. For example, element $I_{3,2} \times P_3$ is equal to the calculated impact for $risk_3$ on $risk_2$ times the calculated likelihood of $risk_3$.

Table 1: Risk Dialog Matrix

Risk (R)	$\mathbf{R_1}$	$\mathbf{R_2}$	$\mathbf{R_3}$	**….**	$\mathbf{R_{n-1}}$	$\mathbf{R_n}$
$\mathbf{R_1}$	$\mathbf{I_1 \times P_1}$	$\mathbf{I_{2,1} \times P_2}$	$\mathbf{I_{3,1} \times P_3}$		$\mathbf{I_{n-1,1} \times P_{n-1}}$	$\mathbf{I_{n,1} \times R_n}$
$\mathbf{R_2}$	$\mathbf{I_{1,2} \times P_1}$	$\mathbf{I_2 \times P_2}$	$\mathbf{I_{3,2} \times P_3}$		$\mathbf{I_{n-1,2} \times P_{n-1}}$	$\mathbf{I_{n,2} \times R_n}$
$\mathbf{R_3}$	$\mathbf{I_{1,3} \times P_1}$	$\mathbf{I_{2,3} \times P_2}$	$\mathbf{I_3 \times P_3}$		$\mathbf{I_{n-1,3} \times P_{n-1}}$	$\mathbf{I_{n,3} \times R_n}$
….						
$\mathbf{R_{n-1}}$	$\mathbf{I_{1,n-1} \times P_1}$	$\mathbf{I_{2,n-1} \times P_2}$	$\mathbf{I_{3,n-1} \times P_3}$		$\mathbf{I_{n-1} \times P_{n-1}}$	$\mathbf{I_{n,n-1} \times R_n}$
$\mathbf{R_n}$	$\mathbf{I_{1,n} \times P_1}$	$\mathbf{I_{2,n} \times P_2}$	$\mathbf{I_{3,n} \times P_3}$		$\mathbf{I_{n-1,n} \times P_{n-1}}$	$\mathbf{I_n \times P_n}$

The third step is to calculate the total risk for each row ($Risk_i$) by adding the values in each element; such value will be called $(total\ risk)_i$. As such the $(total\ risk)_i$ will be calculated as:

$$\mathbf{(Total\ Risk)_i = \Sigma^n_{j=1}(Ij,i \times Pj)}$$

Finally, since different organizations have different risk appetite, the amount of risk exposure that the organization is willing to accept, the risk owner will identify a risk appetite factor from (0 – 1) to be applied to risk dialog to reflect the risk appetite that the management team agreed upon. The appetite risk should be identified and validated by the program risk manager and be communicated with function units of the organization. As such the risk dialog will be calculated as:

$$\mathbf{(Risk\ Dialog)_i = (Risk_i + (Total\ Risk)_{i)} \times RA_i\ ,\ or}$$
$$\mathbf{(Risk\ Dialog)_i = (Risk_i\ Probability\ of\ Occurrence \times Risk_i\ impact\ of\ the\ event + \Sigma^m_{n=1}(I_i \times P_n)) \times RA_i}$$

Where:

$(Risk\ Dialog)_i$ = The total dialog risk for risk i
$Risk_i$ = risk i in a specific function area
I_i = Impact of risk i
P_n = Probability of occurrence of risk n
RA_i = Risk appetite of risk i of the organization (RA_i has a value from 0.0 – 1.0)

The higher the risk score the more serious the risk. At the conclusion of risk prioritization step by a risk dialog formula, a consolidated list of risks is created in the BPC-RMS system to be shared with all functional teams to be used as a foundation for developing and handling control strategies.

In the traditional approaches to risk management, risks are 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. This can be done based on well-known qualitative and quantitative approaches by developing a risk prioritization matrix by using some type of composite probability-impact score (DACS Gold Practice, 2004).

The risk dialog matrix not only provides a holistic view of all risks, but also provides a shared risk knowledge in which integration of risk takes place rather than the narrowly focused linear process presented in traditional risk models. The risk dialog matrix is the second dimension of our multidimensional holistic approach and should be integrated in the BPC-RMS system.

In order to manage and supervise all activities related to BPC-RMS system including the development of the risk dialog matrix we recommend the establishment of a Risk Management Office (RMO), which will develop an enterprise wide program suited to its particular organization. Depending on the organizational structure and culture, different organizations see different implementations for RMPs. For example, a RMO's program can provide one-stop view of risks status, supervise the development and the deployment of common BPC-RMS system, determine skills needed and training focus, and provide a home for career development and advancement. In the next section we describe the proposed RMO responsibilities.

THE RISK MANAGEMENT OFFICE

The proposed Risk Management Office (RMO) is management-centric and the home for planning, designing, implementing, and maintaining the BPC-RMS system including its risk management repository and shared management of uncertainties (Williamson, 2007). The RMO is responsible for creating and maintaining a risk dialog matrix within the BPC-RMS system as described above for the entire organization to help different parties to identify and quantify the impact of one risk in one department on another risk in another department or a function area. In addition, the RMO working with the functional management teams will identify and validate a risk appetite factor to be applied to risk dialog and communicate with function units of the organization.RMO will replace the currently established executive risk committee in some organizations. Some advantages of RMO over the executive risk committee that it will continuously link internal audit, corporate work plan, budgeting (prioritization), and process management. In such a setting, the program established by the RMO will move the function of the executive risk committee from a concept of project and oversight to operational and ongoing functions. This perspective raises risk management structure from a decentralized business unit or functional area responsibility in an ad-hoc basis to an influential role in shaping organizational-wide risk strategies and policies in a shared governance structure.

In addition to a well-built governance system, the proposed Risk Management Office (RMO) should include the following activities: develop policies, procedures, standards and guidelines related to risk management

functions; adopt a common risk management methodology; guarantee exposure identification and analysis mechanisms, document the BPC-RMS system, instigate a formal and standardized incident reporting process, implement a prevention program, implement an emergency response program, prepare/submit a risk management plan, develop an incident follow-up process, a tracking/trending process, review risks and issues, review processes and risk registers, ensure continuous risk reviews to perform a quality assurance role of the risk management system, and staff training/education. Successful Risk Management Office programs will require consistent and detailed processes.

To describe how the RMO program works and for the purpose of this study we will use two main classifications of risks: internal and external. For the external risk we will adopt the PESTLE model (Orange Book, 2004) and for the internal risk we will use what we call the SOFIC model. We now briefly indicate our reasons for this.

Knowing risk categories can provide a structure for organizations to conduct risk assessment by identifying risk and communicating risk information. In addition, classifying risks can help in formulating a risk management plan. Such classification is not meant to establish a hard and fast rule between different types of risks since many risks fall into different categories and one risk in one category may very well have an impact on another risk from another risk category. For instance, a change in foreign exchange rates might have impact on organization's strategy since it may hinder the company's ability to sell internationally.

PESTLE (Political, Economic, Social, Technological, Legal, and Environmental) is well known and is used to analyze change drivers in the external environment. Variants include, for example, Ethics, Education and Demographic factors, which are more organization-specific but would be accommodated as appropriate in our approach. For internal risks, various classifications also exist, of which Strategic, Operational and Financial are central to all enterprises. Factors such as governance, safety and technology may likewise be enterprise-specific and accommodated as required. Whilst various classifications exist, because of increasing general focus on Compliance and the centrality of IT to contemporary organizational activity we add these to the core set used in our illustration. The SOFIC model classifies internal risk categories as: strategic risk, operational risk, financial risk, Information Systems risk, and compliance risk. *Strategic risk* covers the planning, scoping, resourcing and growth of the business; *Operational risk* covers the planning, daily operational activities, product defects, inventory obsolesces, resources (including people) and support required within the a business that results in the successful development and delivery of products/services; *Financial risk* covers cash flow (reduction in income and investment), budgetary requirements (budget overruns), tax obligations, creditor and debtor management, value of tenders and contracts, capital costs change, exchange rate changes, inflation, covenant violation, default on debt, remuneration and other general account management concerns; *Information systems risk* covers the design, implementation, management, maintenance and upgrades associated with technology, recognizing critical IT infrastructure and loss of a particular service/function for an extended period of time, cost benefit associated with technology as part of a business development strategy, and the comparative effectiveness of business processes reliant on designed combinations of people, ICT and enterprise procedures. Finally, *compliance risk* covers legislation, regulations, standards, codes of practice and contractual requirements. Reputation risk is very important and it is included in all the above mentioned risk

categories since if one of the risks become an issue, problem, or crisis it will negatively affect the reputation of the enterprise and public opinion.

To reflect on the "knowledge thinking" and the BPC-RMS system capabilities, the risk Management Office (RMO) approach can best be described through a cog and wheel metaphor, as shown in Figure 3. Rather than the linear process presented in traditional risk models, we propose a holistic program whereby a change in one risk component is supported by other risk components. This approach is reflected in the dialog risk function that we described above. The risk component is integral in ensuring each part of the program interacts appropriately with all other parts of the RMP elements. The ultimate goal is to make the RMO's program a self-improving process that incorporates risk management into the business processes of the organization.

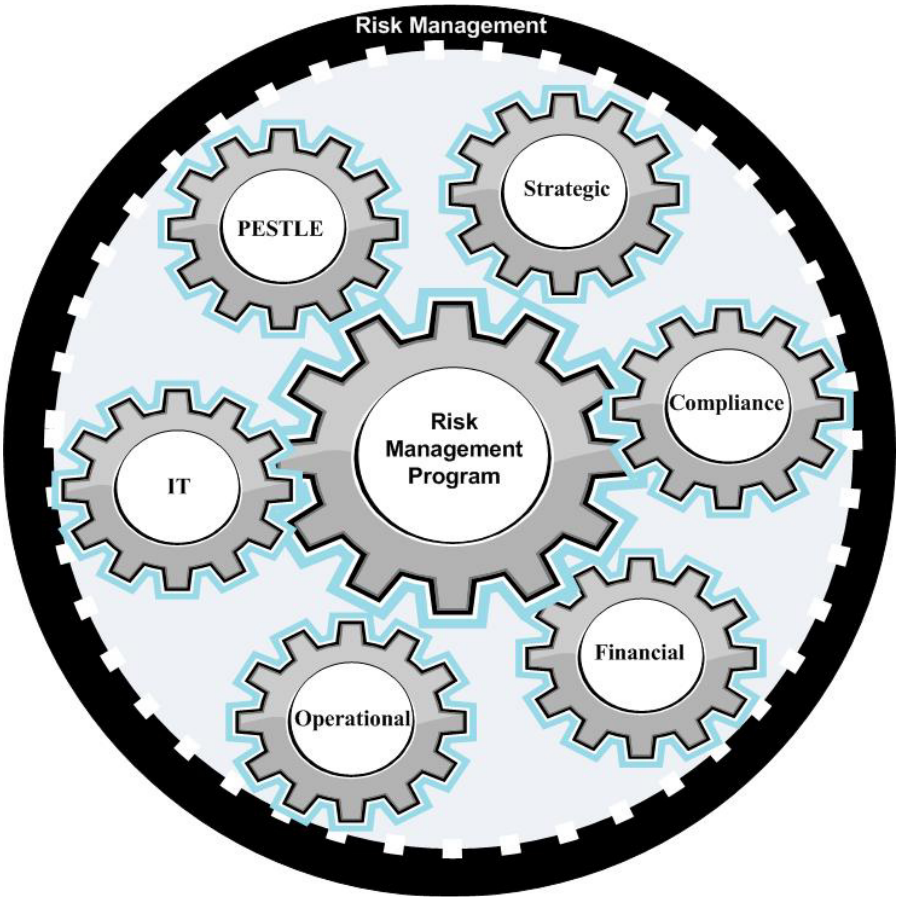

Figure 3: The Risk Management Program Approach

RMP integrates all risk-related activities into a single, comprehensive model that better minimizes risk to an organization, as opposed to the traditional risk model of addressing issues by using a piecemeal approach and making ad hoc decisions.

The RMO will provide assurance to the management team on the effectiveness of risk management within the specific functional area or the firm. Such an office must have the authority working with the risk managers to assign responsibilities to employees and hold them accountable for their actions. As such, the head of the RMO must be a member of the organization's executive team to have such power and to provide risk scrutiny

support to monitor the implementation of the RMO program. In most cases, the head of the RMO will be the Chief Risk Officer (CRO). The RMO will give organizations a visible, repeatable, and consistently applied risk framework and process to support decision making. The RMP approach will give an organization the venue to incorporate all the activities required to assess and control the exposure to any type of risk which may have an impact on the achievement of the organization's business goals and objectives. In addition, the RMO should be aware of the danger of "samethink" and "groupthink" (Janis, 1972) and help organizations to avoid the negative impact of such modes of thinking. Instead, the RMO approach should create a "risk culture" and a "risk knowledge" to avoid these negative modes of thinking.

Our proposed framework requires the establishment of a Risk Management Office as part of the organizational structure and its program should be an integrated part of corporate strategy. The proposed BPC-RMS system is strategically focused and provides the components to be an effective and efficient system for risk management, internal and external auditing, and compliance. The proposed RMO will raise risk management structure from an ad-hoc basis focused on a narrow business unit or functional area responsibility to an influential role in shaping organizational-wide risk strategies and policies in a shared governance structure. By combining BPC-RMS and RMP, they will institute a strong corporate governance to establish an environment for obtaining all risk data from the predefined internal and external resources and by sharing risk knowledge with these trusted resources to assess and control risk associated with their job functions. Such an environment will move focus from "detection after the fact" represented by traditional risk management, to a more preventive identification of fraud and misconduct to meet the organization's goals and objectives.

The six domains and sixteen risk services of the BPC-RMS system will enforce the practice of improving discussions and collaborations between the internal and external stakeholders and help in interchanging risk knowledge in very effective and efficient means. As such and reflecting on the functional emphasis as described above, our framework can be used very effectively for data management, reporting, systems integration, monitoring & tracking, and can be easily integrated into the established financial analysis system that an organization is using. Compiling of risk data and reporting capabilities are provided through the data management capabilities of the BPC-RMS system. Also, the BPC-RMS system integration with other systems within the organization (such as enterprise resource planning) will provide a rich database system that can be used within the structure of the BPC-RMS system to provide background information about the company business. In addition, the alignment of the BPC-RMS with the RMO will give more control on the selection, adoption, and the management of the ERM software packages. Such alignment will give stakeholders very effective monitoring & tracking mechanisms through its powerful risk services and will create a risk culture and focus on strategic sources of risks.

EVALUATION

We developed a questionnaire to assess the practicality of our framework. In order to assess the necessary insight in the practicality of our framework, we developed and administered a survey to risk management practitioners who are members of the ISACA organization in the United Arab Emirates in addition to many executives in the public sector. A total of 67 useable responses were received. Figure 4 presents the industry distribution of the survey respondents. The banking / finance sector represents the largest group followed by

Public services / government / military and retail /wholesale / distribution. 36 percent of the respondents work as internal auditors, 9 percent work as business managers, while 9 percent work as risk managers (see Figure 5).

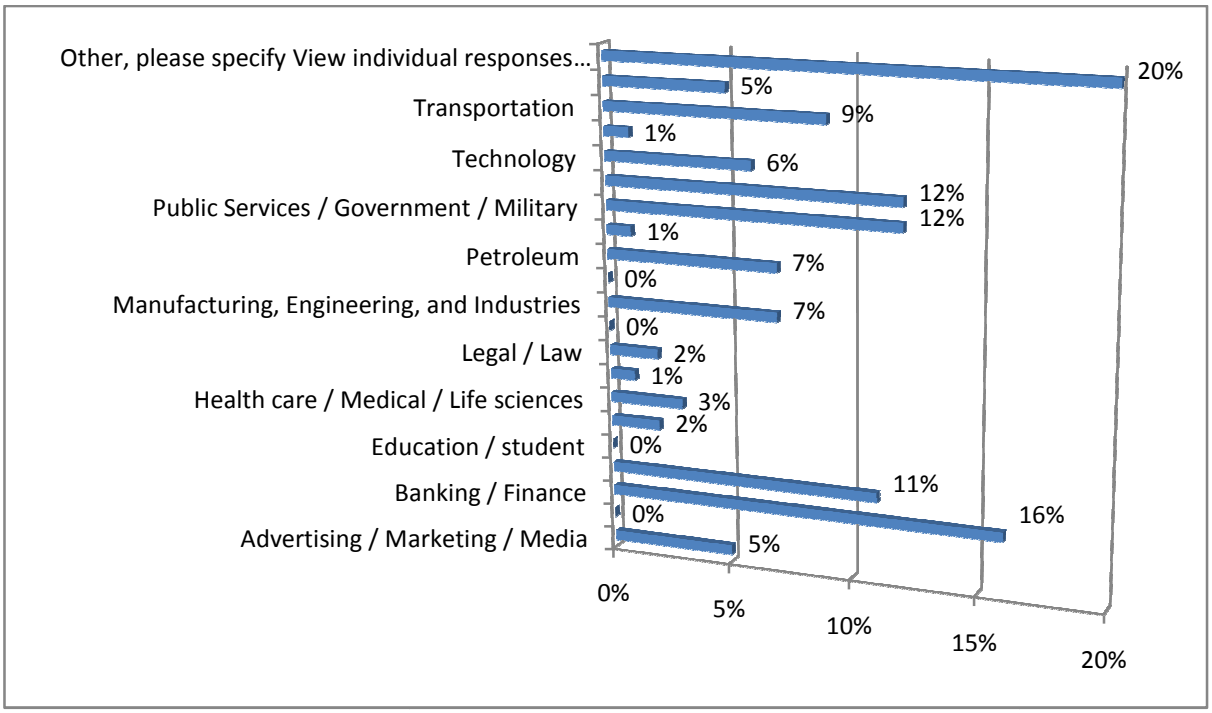

Figure 4: the industry distribution of the survey respondents

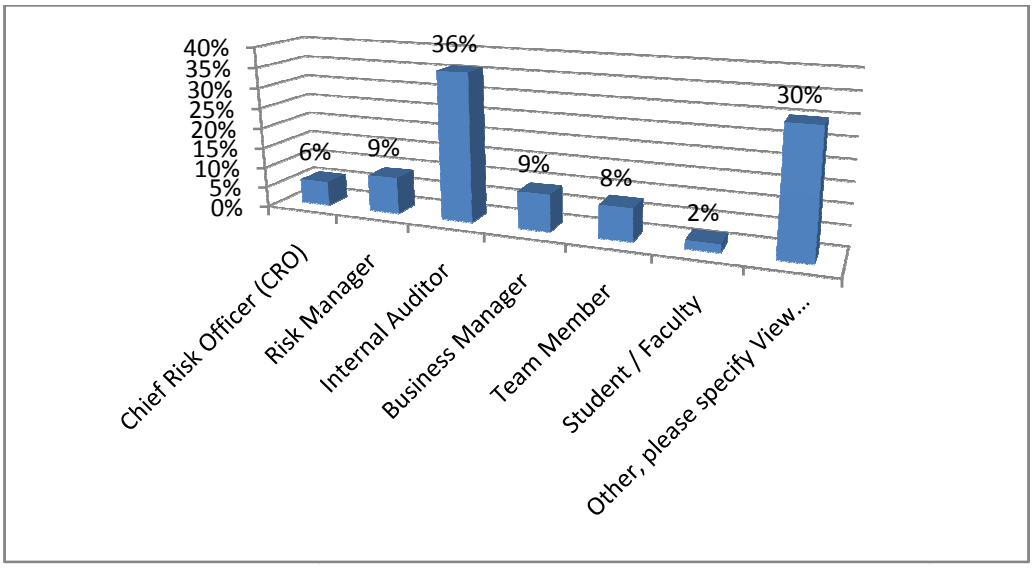

Figure5: The professional positions of the respondents

The participants answer to the question stemmed “Establishing a Risk Management Office (RMO) will help your organization to” are summarized in table 2.

Table 2: Establishing a Risk Management Office (RMO) will help your organization to:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
establish a framework for consistently managing risks through a standard methodology	40.32%	43.55%	12.9%	1.61%	1.61%
define clear lines of responsibility while coordinating people, processes, and tools with one another	40%	41.67%	16.67%	1.67%	0%
avoid both gaps and overlaps between risks and reduce or eliminate duplication of effort	37.29%	50.85%	11.86%	0%	0%
provide better communication	34.48%	56.9%	8.62%	0%	0%
reduce risk management cost	18.18%	41.82%	32.73%	5.45%	1.82%
improve resource management	18.97%	53.45%	24.14%	3.45%	0%
have more accountability	32.14%	53.57%	14.29%	0%	0%
better managing the mitigation strategies	29.09%	56.36%	12.73%	0%	1.82%
have less overhead associated with risk management	12.5%	41.07%	35.71%	8.93%	1.79%
have a common risk repository (database)	37.93%	44.83%	15.52%	0%	1.72%
integrate the risk repository in the business processes of the enterprise	37.93%	44.83%	15.52%	1.72%	0%
maximize risk management efficiency.	42.86%	41.07%	16.07%	0%	0%

The modal response in all cases was to agree or strongly agree and these answers together comprised the vast majority of responses. Thus across a broad range of risk management responsibilities therewas consensus among the professional participants about the importance of establishing risk management office since it will bring a significant value to the enterprise, define clear lines of responsibility, more accountability, avoid both gabs and overlaps between risks, provide better communication, provide significant integration across the functional areas of the enterprise and maximize risk management efficiency.

IMPACT ON PRACTICE AND FURTHER AREAS OF RESEARCH

In the relevance cycle in design science, evaluation considers the designed arte fact against the "utility it contributes to its environment", but for full scientific status evaluation must go further. (Venable et al., 2014). Whilst our initial evaluation suggests that our proposed approach will help in overcoming the challenges and the limitations that practitioners have had in applying the traditional or the enterprise risk management approaches, a fuller reckoning can only occur by longer term assessment of its value in actual practice which is not a matter for controlled experiment. Although an innovative design may be an improvement and evaluated as such to confirm practical relevance, design science as *research* is fulfilled by the "rigour cycle", which considers its general contribution to the knowledge base. As per the analysis discussed earlier in this paper, it is clear that the current practices of risk management lack specific features that our holistic approach addresses. These include setting a consistent level of risk appetite which gives a reliable value across interacting risks, making provision for an enterprise wide view not available to siloed approaches, ensuring a repository for risk knowledge is maintained and current and which allows an enterprise wide risk knowledge sharing culture to evolve, ensuring comprehensive oversight of internal and external risks by an organization-specific program framed within the categories of best practice. An extension to standard risk calculations has

also been formulated to accommodate risk appetite. These contributions are theoretical, but the framework is specified to be practicable.

The proposed framework and solutions is expected to increase the confidence of management in the way functional teams are cooperating when it comes to dealing with risk and will help in increasing the capacity to analyzeinteracting risks in a dialog setting, a potentially measureable indicator. In turn creating risk knowledge and fostering risk-aware culture will increase the success factors of mitigating and responding to all levels of risks. As such, the proposed framework and solutions will have a crucial effect on practice, again a measureable outcome.

As noted, the proposed frame work remains a theoretical contribution, and has not yet been implemented in real world applications. It presents a conceptual framework based on a design science approach but does not include a fuller empirical validation of the framework. Future research should endeavor to validate the framework developed in this study. Another area for research is to develop business process controls for the ABC-PDMS. Such controls will provide assurance about the quality of the data collection process and the accuracy process. Control systems enable management to meet this responsibility.

Further work should attempt to show how integration methods of risk into the business processes used in this study is appropriate across all business processes. One area for research is to develop business process controls for the BPC-RMS. Such controls will provide assurance about the interactions of internal and external entities and the flow of data and information between the domains' components of the BPC-RMS system. Control systems enable management to meet this responsibility. In addition, the rules and responsibilities of the chief risk officer (CRO) should be defined within the framework of the RMO program. Such values will enhance the function of the CRO and provide more power to deal with the board of directors (trustees) and the risk managers within the function areas. Moreover, the newly proposed risk dialog score formula will give meaningful explanation to the values of the integration of risk management and demonstrate the power of opening a formal dialog between all risk managers from all function areas. Such formal dialog will help in providing a detail-oriented approach in which the smaller risks will be treated from analysis point of view equally with more serious risks.

CONCLUSION

The development of enterprise risk management frameworks is an ongoing effort by various organizations and it has an influential role in shaping organizational-wide risk strategies and policies in a shared governance structure. This paper has addressed a number of issues related to the current implementations of enterprise risk management. By using the sciences of design methodology, we have proposed an integration of risk data into the business processes of the enterprise.

The implementation of a well-defined integrated risk management will improve the enterprise business performance and will enhance the value for shareholder by identifying, analyzing, prioritizing, monitoring and controlling all risks across all functional areas that can prevent the enterprise from achieving its set of goals and objectives.

We believe that risk management must be fully integrated with the business processes of the enterprise and be communicated in an effective and efficient manner. We proposed a multidimensional holistic approach which consists of three dimensions: BPC-RMS system, Risk Dialog Matrix, and a centrally led risk management program. In the traditional approaches to risk management, risks are ranked and prioritized as part of risk handling based on the likelihood and the business impact of each risk. The proposed matrix recognizes risk interactions and avoids anomalous values due to linear calculations. The RMP dimension of our approach provides necessary decision support system tools and supports an enterprise-wide approach to ensure an organization's mission is sustained. Whereas Williamson (2007) argued that COSO's command and control approach ignores shared management of uncertainties and social implications of ERM, the risk knowledge and the shared management of risks through RMP is an essential part of our proposal. The holistic approach provides a one-stop view of all risk statuses, develops and deploys a common risk management methodology, accelerates adoption of risk management through training and coaching, and provides systems to integrate risks. This approach to risk management supports the organization's mission by ensuring that no risk activities are stove piped. This paper is one of very first to apply the sciences of design methodology with its three cycles to risk management research and has aimed to provide both a theoretical and a practical contribution. It is hoped this will be of value in the continuing challenge of managing risk.

REFERENCES

Alhawari, S., Karadsheh, L., Talet, A.N., Mansour, E. (2012). Knowledge-Based Risk Management framework for Information Technology project, International Journal of Information Management, 32, (1), pp50-65

Alexander, C., Sheedy, E. (2005). The Professional Risk Managers' Handbook: A Comprehensive Guide to Current Theory and Best Practices. Wilmington, DE, USA: PRMIA Publications; 2005.

Aon Global Risk Consulting (Aon), (2009). "Enterprise Risk Management: S&P Enhancement White Paper. Learn how incorporating a strategic, enterprise-wide approach to risk can enhance your company's credit rating." August 2009.

Ardimento, P. Nicola Boffoli, Danilo Caivano and Marta Cimitile (2011). Towards Knowledge Based Risk Management Approach in Software Projects, Risk Management Trends, Prof. Giancarlo Nota (Ed.), ISBN: 978-953-307-314-9, InTech, DOI: 10.5772/16377. Available from: http://www.intechopen.com/books/risk-management-trends/towards-knowledge-based-risk-management-approach-in-software-projects

Arrow, J. (2008). Knowledge-Based Proactive Project Risk Management. AACE International Transactions (2008): RI11-RI19

Baxter, R., J. C. Bedard, R. Hoitash, and A. Yezegel. 2013. Enterprise Risk Management Program Quality: Determinants, Value Relevance, and the Financial Crisis. Contemporary Accounting Research 30 (4): 1264-1295.

Bofah, K. (n.d.) Portfolio theory explained. eHow. Retrieved on 12/12/11 from http://www.ehow.com/about_5436842_portfolio-theory-explained.html

CFO (2014). The Perils of Silos in Risk Managementhttp://ww2.cfo.com/accounting-tax/2014/05/the-perils-of-silos-in-risk-management/

CGMA (2015). "Global State of Enterprise Risk Oversight 2nd Edition: Analysisof the Challenges and Opportunities for Improvement." Retrieved from https://www.cgma.org/Resources/Reports/DownloadableDocuments/2015-06-13-The-global-state-of-enterprise-risk-oversight-report.pdf

Committee Of Sponsoring Organizations of the Treadway Commission (COSO) (2004). "Enterprise Risk Management – Integrated Framework – Executive Summary." September 2004.

DACS Gold Practice (2004). Document Series GP 12 V 1.0 Formal Risk Management (2004).

Del Bel Belluz D (2010).Announcing the Definitive Risk Management Guidance. Risk Wise E-Zinehttp://riskwise.ca/~riskwise/images/stories/printable/Risk_Management_Made_Simple_E-zine_-_June_2010_Issue.pdf

Del Bel Belluz D (2012).http://www.riskmanagementmonitor.com/the-key-to-an-effective-erm-program/bizculture/

The Economist Intelligence Unit, (2007).Best practice in risk management. A function comes of agehttps://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/best-practice-rm-EIU-0703.pdf

Farrell, M. & Gallagher, R. (2014). The Valuation Implications of Enterprise Risk Management Maturity. Journal of Risk and InsuranceVolume 82, Issue 3, Version of Record online: 10 MAR 2014

Fraser, J. and Simkins, B. J. (2009). Who Reads What Most Often?: A Survey of Enterprise Risk Management Literature Read by Risk Executives, in Enterprise Risk Management, John Wiley & Sons, Inc., Hoboken, NJ, USA. doi: 10.1002/9781118267080.ch22

Gammack JG (1991).Simulating a risk assessor's knowledge for automated decision support In: Shangxu Hu and Shaozhong Jiang (Eds) Information and Systems International Academic Publishers Beijing Vol II p653-657

Gates, S., Nicolas, J.L., WalkerP.L. (2012). Enterprise risk management: A process for enhanced management and improved performance. Management Accounting Quarterly, 13 (3) (2012), pp. 28–38

Harner, Michelle M. (2010). "Barriers to Effective Risk Management," Seton Hall Law Review: Vol. 40: Iss. 4, Article 2. Available at: http://scholarship.shu.edu/shlr/vol40/iss4/2

Hevner, A.R., March, S.T., and Park, J. (2004). "Design Research in Information Systems Research," MIS Quarterly (28:1) 2004, pp 75-105.

Holmes, A. (2002), Risk Management, ExpressExec Module 5.1 Finance, Capstone Publishing, 2002

IT Governance Institute (ITGI), (2007). Control Objectives for Information and related Technology (COBIT 4.1)

The Office on Information Technology Services (ITS) (2007). Enterprise Security and Risk Management Office, "Risk Management Guide", March 09, 2007, Revision 1.7

ISO 31000:2009 Risk Management -- Principles and guidelineshttp://www.iso.org/iso/iso31000

ISO (2009). Guide73 Risk management – vocabulary https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

Janis, Irving L. (1972).Victims of Groupthink. Boston. Houghton Mifflin Company.

Layton, M. and Wagner, S. (2007). "Traditional Risk Management Inadequate To Deal with Today's Threats." March 2007. International Risk Management Institute, Inc. 20 April 2008 <http://www.irmi.com/expert/Articles/2007/Deloitte03.aspx>

Lundquist, A. E. (2014). "Implementing Enterprise Risk Management: Case Studies and Best Practices; CHAPTER 9 Lessons from the Academy ERM Implementation in the University Setting, Western Michigan University". Wiley.

Lundqvist, S.A. (2014). An exploratory study of enterprise risk management: pillars of ERM. Journal of Accounting, Auditing & Finance, 29(3), 393–429

Marks, N. (2011).10 reasons not to like the COSO ERM framework – a discussion with Grant Purdy https://normanmarks.wordpress.com/2011/02/21/10-reasons-not-to-like-the-coso-erm-framework-%E2%80%93-a-discussion-with-grant-purdy/

Majdalawieh, M. (2014). "An Integrated Approach to Enterprise Risk: Building a Collaborative Risk Strategy Within the Business Processes of the Enterprise," ISACA Journal, volume 1, 2014.

Mangram, M. E. (2013). "A SIMPLIFIED PERSPECTIVE OF THE MARKOWITZ PORTFOLIO THEORY". Global Journal of Business Research, Vol 7, Number 1, 2013.

Markowitz, H. M. (1952). Portfolio selection. Journal of Finance, 7(1), 77–91

Massingham, P. (2010).Knowledge risk management: a framework Journal of Knowledge Management 14:3, 464-485

McClure, B. (2010). Modern portfolio theory: Why it's still hip. Investopedia. Retrieved on 12/10/11 from http://www.investopedia.com/articles/06/MPT.asp#axzz1g3JQY7nY.

McKinsey (2013).McKinsey Working Papers on Risk, No. 43Getting to ERM: A road map for banks and other financial institutionshttp://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/Risk/Working%20papers/43_Getting_to_ERM.ashx

McShane, M.K., Nair A., Rustambekov E. (2011). Does Enterprise Risk ManagementIncrease Firm Value, Journal of Accounting, Auditing and Finance, 26(4): 641-658.

Mikes A., Kaplan S.R. (2014) Towards a Contingency Theory of Enterprise RiskManagement. Working Paper. Harvard Business School.January 13, 2014

The Orange Book 2004. "Management of Risk - Principles and Concepts" http://www.hm-treasury.gov.uk/d/orange_book.pdf, October 2004

Pagach, D, Warr, R. (2010). The Effects of Enterprise Risk Management on FirmPerformance. Working paper 27695, Jenkins Graduate School of Management, NorthCarolina State University. April 10, 2010.

Papadaki, K. and Despina,P. (2008). "Collaboration and Knowledge Sharing Platform for supporting Risk Management Network of Practice" The third International Conference on Internet and Web Application and Services, IEEE, 2008pp. 239-244, doi:10.1109/ICIW.2008.78

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2008). "A Design Science Research Methodology for Information Systems Research." Journal of Management Information Systems, 24(3), 34

PWC (2015) "Threat smart: Building a cyber resilient financial institution," PwC FS Viewpoint, January 2015, www.pwc.com/fsi.

Rodriguez, E.& Edwards, J.S. (2014). Knowledge management in support of enterprise risk management International Journal of Knowledge Management, 10(2), 43-61, April-June 2014 43

Shaw, Helen, CFO Magazine, (2006). "The Trouble with COSO: Critics say the Treadway Commission's controls framework is outdated, onerous, and overly complicated. But is there an alternative?" March 15, 2006 http://www.cfo.com/article.cfm/5598405/c_5620756

Stoneburner, G., Goguen, A., &Feringa, A. (2002). Risk Management Guide for Information Technology Systems (NIST Special Publication 800-30). National Institute of Standards and Technology, July 2002.

Talet, A.N.,Alhawari, S. &Karadsheh, L. (2014). The Support of Knowledge Management (KM) Processes to Accomplish Risk Identification (RI) in Jordanian Telecommunication Sector Arab Gulf Journal of Scientific Research (Impact Factor: 0.05). 03/2014; 32(1):26-40.

Venable, J., Pries-Heje, J. and Baskerville R. (2014). FEDS: a Framework for Evaluation in Design Science ResearchEuropean Journal of Information Systems doi: 10.1057/ejis.2014.36

Williamson, D.(2007). "The COSO ERM framework: a critique from systems theory of management control", International Journal of Risk Assessment and Management, Volume 7, Number 8 / 2007, Pgs 1089 - 1119

Woodhouse, P.(2008). "Enterprise Risk Management, BADM 458 – IT Governance" <http://citebm.business.uiuc.edu/TWC%20Class/Project_reports_Spring2008/Business%Risk%20Management/PortiaWoodhouse.pdf>