IDENTIFYING RISKS AND SCENARIOS THREATENING THE ORGANIZATION AS AN ENTERPRISE

Janey V. Camp[1] and Mark D. Abkowitz[2]

Abstract

While risk management has existed for centuries, today it remains a consideration that all too often resides in an organizational silo, associated with planning a new project, evaluating a potential financial investment, complying with new regulations, or responding to a previous incident. Whereas, conceptually it is recognized that risks are inherent within an organization at all levels and in various facets, firms are struggling with how to move toward a more holistic, enterprise-wide approach to risk management. One major challenge is how to structure a framework for identifying enterprise risks and corresponding scenarios that is all inclusive, an important precursor to performing risk assessments and subsequent development of mitigation strategies. This paper reviews the evolution of enterprise risk management (ERM), with a specific focus on risk identification and scenario development. In this discussion, the authors propose an enterprise risk identification framework, one that is representative of all potential threats to the enterprise, yet practical in its use.

Keywords: enterprise risk management, risk identification, risk scenarios, risk management, operational risk management

[1] Research Associate, Department of Civil and Environmental Engineering, Vanderbilt University, VU Station B 351831, 2301 Vanderbilt Place, Nashville, TN 37235-1831USA. Tel: +1615 322 2739; Fax: +1615 322 3365. E-mail address: janey.camp@vanderbilt.edu

[2] Professor, Department of Civil and Environmental Engineering, Vanderbilt University, VU Station B 351831, 2301 Vanderbilt Place, Nashville, TN 37235-1831. USA. Tel: +1615 322 3436; Fax: +1615 322 3365. E-mail address: mark.d.abkowitz@vanderbilt.edu

IDENTIFYING RISKS AND SCENARIOS THREATENING THE ORGANIZATION AS AN ENTERPRISE

Janey V. Camp and Mark D. Abkowitz

Janey V. Camp, Department of Civil and Environmental Engineering, Vanderbilt University, VU Station B 351831, 2301 Vanderbilt Place, Nashville, TN 37235-1831USA. Tel: +1615 322 2739; Fax: +1615 322 3365. E-mail address: janey.v.smith@vanderbilt.edu

Mark D. Abkowitz, Department of Civil and Environmental Engineering, Vanderbilt University, VU Station B 351831, 2301 Vanderbilt Place, Nashville, TN 37235-1831. USA. Tel: +1615 322 3436; Fax: +1615 322 3365. E-mail address: mark.d.abkowitz@vanderbilt.edu

Introduction

Risk management is becoming more commonplace in both the private and public sector as part of daily operations. To date, however, this practice has been typically performed in organizational "silos", often focused on the planning phase of a new project (Akintoye and MacLeod 1997; Dey 2009), when considering a potential financial investment, to comply with new regulations, or in response to a previous incident (Smithson and Song 2004; Gates and Hexter 2005; O'Donnell 2005; Crouhy, Galai et al. 2006; Nocco and Stulz 2006). Moreover, there has been little consistency in the use of risk management techniques across differing industry sectors or between organizations in the same sector, with the exception of a general consensus that risk management is important for business survival (Gates and Hexter 2005; Kennedy 2005).

The intent of this paper is to review recent developments in risk identification that are impacting the emergence of enterprise risk management (ERM) as a business practice. This review is meant to serve as a guide in the development of a risk identification framework, including corresponding scenarios, that addresses *all* potential threats to an organization's livelihood. A proposed framework that meets this objective is subsequently presented by the authors.

Background

Risk management has existed for centuries, beginning as far back as the *Code of Hammurabi* (Covello and Mumpower 1985). Throughout history, while not necessarily

termed as such, risk management has embodied pollution, transportation, natural disasters, personal liability, building and fire codes, human health, and food safety. Trammell (2004) captures this evolution in his statement that the goal of risk management is to protect workers, the community, the environment, customers, and the organization's physical assets.

Today, in light of a spate of recent natural disasters, large-scale accidents and malicious acts, enterprise risk management (ERM) has become a favorite expression among organizations in both the private and public sector. Consequently, many organizations have instituted what they believe to be ERM as part of daily operations. Gates and Hexter (2005), in surveying 271 financial and risk executives, reported that over one-half of respondents (56%) are making efforts to develop and implement some form of "enterprise risk management" strategies within their organizations, with another 35% of those surveyed positively disposed towards using ERM. Corporate governance, regulatory requirements, and an increased understanding of strategic and operating risks are motivating ERM implementation in these organizations (Gates 2006).

Scope of Enterprise Risk Management

While many firms are utilizing the term *enterprise risk management*, their approaches range from managing risks for a specific purpose to a company-wide implementation involving the commitment of considerable financial and human assets (Lam 2000; Nocco and Stulz 2006). In reality, it is only the holistic approach, one that includes all risk-

related events, processes, and decisions, internal and external to the firm, which deserves the ERM label. The intent of the following discussion is to help clarify this distinction.

In many instances, risk management is considered when a change is taking place in an organization. The "enterprise" could be a new acquisition, merger, or simply the beginning of a new initiative. This project-centric form of risk management becomes even more limiting when one considers that identified risks can often be as narrowly-defined as those that impact a single activity's schedule or cost (Akintoye and MacLeod 1997).

Such has often been the case in the financial sector, with the metric being a monetary expression of the risk/reward associated with a particular investment strategy (Stulz 1996). However, given the banking industry's recent upheaval, risk is becoming recognized as more than just accounting for financial losses due to unexpected events. It now extends into more transparent disclosure, motivated by the need to comply with recent requirements imposed by the likes of Sarbanes Oxley and Basel II. Both of these protocols are designed to help prevent future large-scale losses while protecting individual investors from exceptionally risky decisions and unethical practices associated with overzealous investment managers. As a result, the financial sector is gravitating towards a more holistic, and appropriate, view of ERM.

Operational risk management (ORM) extends beyond the financial aspects of risk, to include inefficiencies or failures of the people, processes and systems that are essential to

survival and functionality of an organization. ORM has become a popular term, one that is often misconstrued as financial risk management or as ERM, when it is more comprehensive than the former but less than the latter.

Enterprise risk management is used synonymously with the terms holistic risk management, integrated risk management, and strategic risk management (Hoyt, Dudley L. Moore et al.). A holistic approach enables an organization to manage a vast array of risks in an integrated, enterprise-wide fashion, where increased awareness throughout the entire organization emerges, leading to better coordination and thus improved decision-making. To emphasize this point, Gates and Hester (2005) define ERM as a *comprehensive* approach for evaluating activities and assessing risks associated with conducting business.

To date, there been a paucity of literature devoted to the process and application of enterprise risk management. This is burdened in part by literature claiming to discuss ERM that is actually focused on operational or project risk management, leading to much confusion among practitioners. Given these circumstances, it is important to place ERM in an appropriate context and to develop a framework that enables true enterprise risks to be identified and placed into a workable structure. This is the basis for the following discussion.

Enterprise Risk Identification

Historically, risk identification has been heavily influenced by known problems or prior incidents. This reactionary mode typically limits the amount of creative thought that is invested in identifying all potential scenarios of what could go wrong. Fortunately, many organizations are evolving towards a more proactive approach by assembling organizational teams and utilizing outside expertise to recognize risks to the enterprise. One popular approach is to identify risks through compartmentalization, that is focusing on each process, department or organizational group as a unique entity (COSO 2004; EPCB Accessed December 2009). Often, risks are characterized as internal or external in origin, consistent with the level of organizational control; Dey (2009) classifies these as business (external) risks and operational (internal) risks. Another approach is to group risks into those that are more closely associated with individuals and those that belong more to the organization (Reason 2004). Finally, there is the multi-level concept, where risk is identified as residing at the enterprise, division, subsidiary, and/or business unit level (COSO 2004).

Given the differences in these approaches, it is not surprising that a variety of ERM risk categories have emerged (see Table 1). For example, the list of risks compiled by Covello and Mumpower (1985) contains natural disasters, epidemic disease, pollution, food contamination and adulteration, building failure, fire, transportation accidents and occupational injuries. Each of these categories became a focus for government intervention to protect the public, in response to a significant event that occurred that raised awareness and required a response. In contrast, Dey (2009) identifies risk in the

construction industry as being either market, financial, economical, environmental and social, or technological and political in nature. While market, financial and economic risks could be arguably consolidated into a single economic risk category, Dey completely ignores employee health and safety, which one would expect to be a large risk component of a construction project. The American Institute of Certified Public Accountants (AICPA) Committee of Sponsoring Organizations of the Treadway Commission's ERM framework suggests four risk categories: 1) strategic, 2) operations, 3) reporting, and 4) compliance (COSO 2004). This grouping is heavily weighted toward those risks where the organization is held accountable by an external authority. Meanwhile, Deloitte, a leader in the enterprise risk consulting industry, defines ERM risk as being regulatory, technical, price or market, physical operations, volume, modeling or valuation, or human capital oriented, presenting a more holistic approach (Concessi and Curtis 2008).

A slightly different approach is to categorize risk in terms of the recipient, whether it be workers, customers, the community, the environment, or an organization's physical assets (Trammell, Lorenzo et al. 2004). A modification of this approach is to identify risk according to "upstream factors" that lead to incidents, resulting in risk categories of individuals, the workplace, the organization, regulators, and society at large (Reason 2004).

In summary, while there is a lack of consistency in how enterprise risks have been identified and categorized, there is general agreement that enterprise risks encompass a

variety of considerations, both inside and outside of an organization, affecting numerous stakeholders. This is an encouraging sign in terms of the potential for creating a uniform risk identification framework that can serve as the basis for establishing an ERM practice for any organization.

Enterprise Risk Identification Tools

A variety of software tools have been marketed as being able to support risk identification from an enterprise perspective (see Table 2). Upon closer inspection, however, capabilities are often limited to risks arising out of claims and regulatory compliance, or tracking of risks associated with managing project costs and schedule. It is notable that few tools focus on striving to identifying enterprise risks in a holistic, integrated manner.

INSERT TABLE 1 HERE.

RISKMASTER™ is an example of claims tracking software (CSC Accessed October 2009). It supports management of data related to property, general and professional liability, worker compensation, accidents, injuries, disabilities, and automotive liability. Information about each event is stored for later use in managing a claim or performing analyses of trends and loss patterns. While RISKMASTER™ provides many capabilities for logging different types of risk events, it does not assist in identifying hazards where no detrimental event has previously occurred. Other software packages with similar capabilities include RiskConsole (Aon Accessed November 2009), RiskCheck

(RiskCheck Accessed November 2009), and Claims Management Software and Enterprise Incident Register™ (NOWECO Accessed 2009).

A tool developed to assist with compliance risk management is CompliantPro (IBS Accessed September 2009). It is used to help organizations meet regulatory requirements and guidelines associated with ISO 9001:2008 (Quality Management Standard); ISO/TS 16949 (Automotive Quality Standard); ISO 13485 (Medical Device Standard); FDA 21 CFR Part 11 (Electronic Records); FDA 21 CFR Part 820 (Quality System Regulation); ISO 14000 (Environmental Management Standard); BS 8800/OHSAS 18000 (Health & Safety Management System); and the Sarbanes Oxley Act. This too falls short of a completely holistic approach to enterprise risk management given an orientation solely devoted to meeting regulatory requirements and quality standards.

With regard to project risk management software, RiskTrak™ is one of the more comprehensive commercially available software packages. It supports the evaluation of risk influences on both project costs and schedule. RiskTrak™ utilizes a four-step risk assessment method, IDEA™ (identify, define, estimate, and analyze). Electronic questionnaires are used to guide the risk assessment process (RiskTrak Accessed November 2009). Another project risk management tool is part of a suite of software products contained within the Enterprise Risk Register™ (NOWECO Accessed 2009). While the product name implies that this software is useful for the entire enterprise, it is merely an accounting tool, where the responsibility lies with the user to identify and log all risks before an assessment can be performed.

One of more promising enterprise risk identification tools is the Vulnerability Assessment Workbook (EPCB Accessed September 2009). This Excel-based product focuses on a facility-wide basis, where the user is provided with a list of potential hazardous events to consider in assigning a risk score based on the likelihood of occurrence and potential consequences. The hazards are separated into the following event groups: natural, technological/industrial, and civil/political. While this application offers an approach to anticipating risk-based scenarios, the Vulnerability Assessment Workbook is limited to considering primarily external hazards (e.g., 15 of the 34 hazard events listed are weather-related) and the tool only provides general guidance (i.e., template) for performing risk identification.

INSERT TABLE 2 HERE

Room for Improvement

As noted in the previous discussion, there is a growing appreciation, both among organizations trying to manage their risks and third-parties developing tools to assist in these efforts, for the need to address risk management as an enterprise-wide program, represented as a holistic and integrated process. While simple in concept, putting this into practice has proven to be more difficult. All too often, portions of enterprise risk are "owned" by different parts of the organization with little interaction between silos or integration at the highest levels within the entity. While attempts are being made to identify enterprise risks and construct appropriate event scenarios for analysis, there is little agreement over what they are or how they should be classified. The situation calls

for a fresh approach to overcome these shortcomings, which is the subject of the following discussion.

A New Enterprise Risk Identification Framework

The first step in developing an improved framework for identifying enterprise risks is to develop a set of risk categories that is holistic in nature, but can be segmented into specific risk areas that are intuitively appealing and practical to apply. Figure 1 presents a proposed structure for accomplishing this objective.

INSERT FIGURE 1 HERE

In this framework, risks are grouped into categories, first by whether they are considered internal or external in nature. The terms “internal” and “external” identify the origin of the hazard with respect to the organization in addition to providing an indication of the extent to which an organization can control the referenced risk. Some risk categories can be associated with both internal and external risks; however, the hazards that fall into these categories would be different. For example, an information security breach that originates as a computer virus sent by an email to an employee would be considered an external risk, whereas an employee copying files or stealing proprietary company information for personal gain would be considered an internal risk, even though both events involve information breaches that compromise the organization’s intelligence and data systems.

Beyond the division of internal and external risks, the proposed framework is segmented into three principal categories: 1) operational, 2) information systems, and 3) physical. Operational risks are defined as those that relate to how business is transacted within the organization. These include risks associated with financial decisions, resource management, and relationships with employees, contractors and customers. Information system risks include computer hardware and software, as well as all "intangible" assets associated with those systems (i.e., data, employee personal information, bank records, and customer accounts). Among an organization's physical assets are buildings, stock and equipment. Employees and their well being (i.e., health and safety) also falls into this category, along with those risks associated with environmental releases by the organization or by others (external) that may adversely impact business operations.

The aforementioned categories comprise a generalized framework for consideration of "all" risks. In previous literature, while a number of different risk categories have been put forward, they have generally lacked this top-down, enterprise-wide perspective. As a validation exercise, the authors attempted to place each risk previously appearing in the literature into one of the categories in the proposed framework. This proved successful in all cases. For example, Trammell, et al. (2004) includes workers, community, environment, customers, and the company's physical assets. These would be placed in the proposed framework categories of internal - employee health and safety, external – social, political and economic relations, either internal – environmental releases or external – environmental and natural hazards (depending on the focus), external –

customer, supplier, and off-site contractor relations, and internal – facility, infrastructure and physical assets, respectively.

Within each risk category reside a number of different hazards that can threaten the organization. For example, in the External – Physical – Environmental & Natural Hazards category, hazards could include tornadoes, earthquakes, floods, wildfires, and heavy snowfall and many others. Because the events associated with each hazard will differ, it is important to capture these circumstances in terms that can easily be envisioned for consideration and analysis. The most promising format for doing so is development of event scenarios for each hazard.

Scenario Development

Once enterprise risks have been identified and categorized, an important next step in performing ERM is the ability to define scenarios to which event likelihoods and consequences can subsequently be assigned (Jablonowski 1999). The lynchpin to this process is ensuring that each reasonably foreseeable scenario for each hazard with each enterprise risk category has been considered.

To fully understand the potential risks associated with each hazard, multiple scenarios must be evaluated. These scenarios should represent the range of events that are "reasonably foreseeable" that an organization may experience. The basis for determining these event scenarios is based on answering the question, "What could go wrong?" To capture the full breadth of possibilities, the developed scenarios should represent

incremental levels of impact severity, ranging from events with minor to catastrophic outcomes. Referring to the previous discussion, for a tornado hazard, at one end of the spectrum, a scenario might be a tornado warning for a two-hour window during the business day in the county where the organization is situated, although a tornado does not subsequently materialize. On the other end of the scenario spectrum might be a direct hit to the facility of interest by an F4 tornado that completely destroys the building and causes human casualties. Of course, other scenarios can be constructed to represent tornado events that fall in between these two extremities.

It is important to distinguish the creation of event scenarios from their likelihood of occurrence. Assigning these probabilities comes at a later stage in the risk assessment process. What is critical at this stage is that all reasonably foreseeable risks have been identified and characterized in the form of scenarios for each hazard in each of the ERM framework categories. Therefore, as the risk assessment process progresses, one has confidence that the organization will experience no surprises because it was systematic and comprehensive in how it approached risk identification.

Concluding Remarks

In this paper, we have reviewed the state-of-the-art in identifying and categorizing risks that could threaten an organization as an enterprise. In doing so, it became apparent that while recent trends have been moving towards a more holistic, integrated approach to risk management, a consistent framework for identifying risks and corresponding scenarios so as to enable true enterprise risk management has yet to emerge.

To overcome these limitations, an improved framework for classifying enterprise risks was proposed. Within this framework, applicable enterprise risks can be identified, leading to the formulation of scenarios involving each risk that are considered to be "reasonably foreseeable".

Once this step is complete, each risk scenario can be subjected to an assessment of its likelihood and consequence, leading to risk prioritization and development of cost-effective mitigation strategies. The authors are currently developing this aspect of the ERM methodology.

By moving research and development in this direction, a more comprehensive, yet practical basis for performing ERM can evolve, one that will help enable ERM to become a core business practice in any organization.

ACKNOWLEDGEMENTS

The research described herein was sponsored by funds from the Intermodal Freight Transportation Institute at the University of Memphis through the federal Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU), and by an unrestricted gift to Vanderbilt University from the Ingram Barge Company. The authors are grateful for this support as well as the assistance provided by affiliated individuals in the performance of project activities.

REFERENCES

Akintoye, A. S. and M. J. MacLeod (1997). "Risk Analysis and Management in Construction." International Journal of Project Management **15**(1): 31-38.

Aon (Accessed November 2009). RiskConsole. Aon Risk Management, Reinsurance, Human Capitol Consulting. http://www.aon.com.

Concessi, P. and P. C. Curtis (2008). "The Risk Intelligent Energy Company: Weathering the Storm of Climate Change." Oil and Gas Financial Journal: 1-4.

COSO (2004). Enterprise Risk Management - Integrated Framework. . New York, NY, Committee of Sponsoring Organizations of the Treadway Commission (COSO), American Institute of Certified Public Accountants (AICPA).

Covello, V. T. and J. Mumpower (1985). "Risk Analysis and Risk Management: An Historical Perspective." Risk Analysis **5**(2): 103-120.

Crouhy, M., D. Galai, et al. (2006). The Essentials of Risk Management. New York, New York, McGraw Hill.

CSC (Accessed October 2009). RISKMASTER(R). Computer Services Corporation. http://www.csc.com/services.

Dey, P. (2009). "Managing Risks of Large Scale Construction Projects." Cost Engineering **51**(6): 23-27.

EPCB (Accessed December 2009). Complete Continuity Toolkit. EPCB Risk Management Consultants. www.emergencyriskmanagement.com.

EPCB (Accessed September 2009). A Tailorable Diagnostic Tool. Emergency Preparedness Capacity Builders. www.emergencyriskmanagement.com.

Gates, S. (2006). "Incorporating Strategic Risk into Enterprise Risk Management: A Survey of Current Corporate Practice." Journal of Applied Corporate Finance **18**(4): 80-91.

Gates, S. and E. Hexter (2005). "The Strategic Benefits of Managing Risks." MIT Sloan Management Review.

Hoyt, R. E., J. Dudley L. Moore, et al. (2008). "The Value of Enterprise Risk Management: Evidence from the U.S. Insurance Industry." Society of the Actuaries: 1-22.

IBS (Accessed September 2009). CompliantPro. www.ibs-us.com.

Jablonowski, M. (1999). "Scenario-Based Risk Analysis." Disaster Recovery Journal: http://www.drj.com/drworld/content/w3_034.htm.

Kennedy, D. (2005). "Risks and Risks." Science **309**(5744): 2137.

Lam, J. (2000). "Enterprise-wide Risk Management and the Role of the Chief Risk Officer." ERisk.com: 1-5.

Nocco, B. W. and R. M. Stulz (2006). "Enterprise Risk Management: Theory and Practice." Journal of Applied Corporate Finance **18**(4): 8-20.

NOWECO (Accessed 2009). RiskDecision Risk Management Software. Northwest Controlling Corporation, Ltd. http://www.noweco.com/emse.htm.

O'Donnell, E. (2005). "Enterprise risk management: A systems-thinking framework for the event identification phase." International Journal of Accounting Information Systems **6**: 172-195.

Reason, J. (2004). Managing the Risks of Organizational Accidents. Cleveland, OH, RMC V. http://rmc.nasa.gov/archive/rmc_v/presentations/reason%20managing%20the%20risks%20of%20organizational%20accidents.pdf.

RiskCheck (Accessed November 2009). Risk Check Software. www.riskcheckinc.com.

RiskTrak (Accessed November 2009). RiskTrak Consulting and Software. www.risktrak.com.

Smithson, C. and P. Song (2004). "Quantifying operational risk." Risk Class Notes: 50-52.

Stulz, R. M. (1996). "Rethinking Risk Management." Journal of Applied Corporate Finance **9**(3): 8-24.

Table 1: Sample Enterprise Risk Categories

Author	Year	Enterprise Risk Categories
Concessi and Curtis (Deloitte)	2008	* Regulatory, Technical, Price/Market, Strategic, Physical Operations, Volume, Modeling/Valuation, Human Capital
Hoosaian	2003	* People, Process, System, External Party/Event
Diligence (Risk Consulting)	Accessed 2009	* Transaction, Brand & Reputation, Competitive, IT, Fraud, Intellectual Property, Personnel, Physical, Regulatory, Political
Cuvello and Mumpower	1985	* Natural Disasters, Epidemic Disease, Pollution, Food Contamination and Adulteration, Building Failure, Fire, Transportation Accidents, Occupational Injuries
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	2004	* Strategic, Operations, Reporting, Compliance
Miller and Waller	2003	* Industrial Uncertainties, Firm-Specific Uncertainties
Dey	2009	* Market, Financial, Economical, Environmental and Social, Technological, Political
Kaplan, Haimes and Garrick	2001	* Modal, Information Management, Functional, Geographical/Spatial, System, User/Stakeholders, Management
Roberts	2001	* Plans, Processes, Procedures, Requirements, Integrated Master Plan and Schedule, Costs
Trammell, Lorenzo and Davis	2004	* Workers, Community, Environment, Customers, Physical Assets
US Department of Transportation FHA International Programs (Caltrans Sample Risk List)	Accessed 2009	* Technical, External, Environmental, Organizational, Right-Of-Way, Construction, Regulatory
US Department of Transportation FHA International Programs (WSDOT 2002 Urban Corridors Common Risks)	Accessed 2009	* Economic, Environmental, Third Party, Right-Of-Way, Management, Geotechnical, Design Process, Construction

Table 2: Sample Enterprise Risk Identification Tools

Company	Risk Software	Features
RiskTrak International	RiskTrak™	* Project focused; Questions provided for user interview without real risk identification guidance; User can import/export project files
Computer Sciences Corporation (CSC)	RISKMASTER®	* Incident and claim tracking (worker compensation, disability, property and liability)
SAP	SAP® Business Objects™	* Manages governance, compliance, and other risks in an organization-wide approach; Tracks reporting and audit trails
IBS	CompliantPro™	* Enterprise-wide compliance management; Standards include quality management, automotive quality management, medical devices, electronic records, environmental management, health and safety management, Sarbanes Oxley Act
Strategic Thought	Active Risk Manager (ARM)	* Began as a project and program risk management tool; Newer versions have some enterprise risk management capabilities; Works with 3rd party project and planning applications; Includes limited risk identification and assessment
NOWECO	Enterprise Risk Register®	* Operational risk accounting (people, property, processes, business continuity, reputation, and environment); Tracks risks by department, division, location, project or asset; Supports compliance standards including Basel II, Sarbanes Oxley Act, COSO, Risk Management Standard, AS/NZS 4360 and KonTraG
Northwest Controlling Corporation, Ltd. (NOWECO)	RiskDecision	* Project or business plan risk manager; Allows for quantitative or qualitative risk assessment; Provides user-defined categories, work breakdown structure and timelines
Syntex Management Systems, Inc.	IMPACT ERM®, IMPACT Enterprise®, IMPACT Anywhere®	* Web-based design for enterprise-wide operational risk management; Provides incident management, risk audits, and corporate compliance management with reporting options and performance analytics; Focused on risk/loss identification at field-level work processes
methodware ™	methodware™	* Includes tools for risk auditing, compliance and governance
Aon	RiskConsole	* Set of integrated modules for incident, claims, property, fleet, litigation, policy, and property risk control; Considers the organizational hierarchy for operations management; Browser-based tool; Primarily focused on hospital and physician liability; Consolidates data from payroll and human resources; Includes a risk register module for recording and tracking risk information
EPCB	Vulnerability Assessment Workbook	* Sample vulnerability assessment tool with risk identification and scoring worksheet; Hazards provided include natural, technical/industrial, civil/political events; Scores are used to plot risks on heat map; Provides qualitative assessment assistance and color-coded risk rankings; Questionnaire

		evaluates business impact vulnerability
Palisade	@RISK, RISKOptimizer	* Focused on financial management, including inventory, markets, cash flows, purchases and retirement planning

Figure 1: Proposed Enterprise Risk Categories