

PERSPECTIVE

STRUCTURING AN ENTERPRISE RISK ASSESSMENT PROTOCOL: TRADITIONAL PRACTICE AND NEW METHODS

Mark Abkowitz
Janey Camp

ABSTRACT

In a world that has become increasingly complex, enterprise risk management (ERM) has emerged as a practice for identifying reasonably foreseeable hazards that pose risks to an organization, both its physical and human assets. Due to the breadth and depth of factors that can impact an organization's risk portfolio, it is incumbent that the underlying risk assessment process that supports ERM embodies a holistic and systematic approach. This is easier said than done, however, as much of the effort in self-acclaimed ERM programs remain entrenched in compartmentalized parts of the organization or ignore threats that are "outside of the box" of the operating environment to which management is accustomed. This environment therefore creates opportunities for key risks to go unnoticed. The authors propose a comprehensive, yet flexible framework for overcoming this challenge, an approach that can be utilized by both the public and private sector. A sample application is provided, using a free, web-based tool developed as part of the initiative.

INTRODUCTION

Risk is inherent within any organization, at all levels and in various facets. Such is the nature of the risk versus reward trade-off that represents life as we know it. It should therefore come as no surprise that the concept of risk management has existed for centuries, dating back as far as the Code of Hammurabi. Throughout history, risk management has embodied considerations that include pollution, transportation, natural disasters, personal liability, building and fire codes, human health, and food safety (Covello and Mumpower, 1985). However, today's risk world has become increasingly complex due to global competition, dependency on international supply chains, political instability, climate change, and technological innovation. It demands broader perspective when it comes to identifying, characterizing, and assessing risks that may threaten an organization. This has motivated many organizations to consider implementing enterprise risk management (ERM) as a core business practice.

Mark Abkowitz is at Vanderbilt University, Civil and Environmental Engineering, 400 24th Avenue South, Jacobs Hall, Room 292, Nashville, TN 37235. Abkowitz can be contacted via e-mail: mark.abkowitz@vanderbilt.edu. Janey Camp is at Vanderbilt University, Civil and Environmental Engineering, Nashville, TN 37325. Camp can be contacted via e-mail: janey.camp@vanderbilt.edu.

In this article, we define ERM as:

... a *systematic approach* enabling an organization to consider *all factors* that threaten its ability to meet *business objectives* and implement appropriate *risk management controls* according to the organization's *risk appetite*.

Certain terms have been italicized in this definition because they connote an important message. A “systematic approach” implies that there is an overarching structure to the risk management process. Consideration of “all factors” emphasizes the need to cast the net widely to ensure that all hazards, which can potentially threaten the organization, have been identified. Reference to “business objectives” recognizes that each enterprise has its own measures of success upon which it is judged. The implementation of “risk management controls” defines what the organization believes are cost-effective mitigation strategies. Reference to the enterprise’s “risk appetite” acknowledges that each enterprise has a different risk tolerance, which will guide whether a certain risk is deemed acceptable or requires a mitigation action.

ERM as a concept was introduced in the early 1990s by Miller (1992), although it took a period of time thereafter for the idea to take root (Kleffner et al., 2003; Liebenberg and Hoyt, 2003). The maturation of ERM practices also brought a greater appreciation for the complexities involved in implementing an integrated risk management program as well as the roles and responsibilities of risk champions.

By the turn of the century, a critical mass of firms was pursuing this concept. As noted by Gates and Hexter (2005), in surveying 271 financial and risk executives, the vast majority were either making efforts to develop and implement ERM strategies within their organizations, or were positively disposed toward using ERM. Concurrently, organizations involved in establishing industry codes and standards began developing guidelines for formulating and implementing an ERM practice (Committee of Sponsoring Organizations of the Treadway Commission, 2004; Australian/New Zealand Standard, 2004).

More recently, a global risk management study conducted by Accenture reported that over 80 percent of corporate-level executives surveyed viewed risk management capabilities as critical for dealing with management volatility and organizational complexity (Accenture, 2011). These executives were associated with nearly 400 companies representing 10 industry sectors, operating in several continents. The publication of ISO 31000 was designed for guidelines to keep pace with this uptick in ERM interest and application (International Organization for Standardization, 2009).

Much of the excitement around ERM as a management practice stems from an appreciation for the value it brings to the financial health of the organization (Hoyt and Liebenberg, 2011; Pagach and Warr, 2011). This has stimulated interest in strategic investments in ERM with an eye toward improving the bottom line (Ai et al., 2012). The opportunities that can be derived from an effective ERM program include: (1) enhancing the safety and security of employees, business partners, and the community at large; (2) improving the quality of decisions and reducing surprises by being better risk informed; (3) controlling unnecessary expenditures by treating risks before they become more costly problems; (4) creating opportunities for competitive advantage; (5) helping to grow a proactive organizational culture that recognizes and rewards problem avoidance; and (6) increasing stakeholder confidence by demonstrating good stewardship. It

should therefore come as no surprise that the number of studies examining financial characteristics of companies adopting ERM, determinants of ERM adoption, ERM practices, impact of ERM on firm performance, and ERM organizational leadership have proliferated of late (Togok and Zainuddin, 2014).

ENTERPRISE RISK ASSESSMENT

At the heart of any successful ERM practice is the ability to identify all potential threats to the organization's well-being and to correctly assess the likelihood and consequence of its occurrence. Often referred to as the "risk triplet," the enterprise risk assessment process consists of addressing three sequential questions (Oryang, 2002):

1. What can go wrong?
2. How likely is it?
3. What are the consequences?

An enterprise risk assessment protocol encompasses the steps involved in addressing the risk triplet (Holmes, 2002; Health Service Executive, 2009).

Historically, there has been little consistency in the use of risk assessment protocols across different industry sectors or between organizations within the same sector (Gates and Hexter, 2005; Kennedy, 2005). Moreover, some organizations have chosen to only engage its use during the planning phase of a new project, when evaluating a potential financial investment, to comply with a government regulation, or in response to a previous incident in which significant losses were incurred (Smithson and Song, 2004; O'Donnell, 2005; Crouhy et al., 2006; Nocco and Stulz, 2006; Dey, 2009). Even when the intent has been more broadly based, assessment of risks potentially afflicting the enterprise has often been compartmentalized and independently evaluated.

Much of the difficulty in developing an effective enterprise risk assessment protocol can be attributed to the argument that while conceptually the process may appear straightforward, in practice, it can be quite cumbersome. The first step, identifying what can go wrong, is particularly challenging. The danger in not doing this properly is that the organization believes that it is aware of all potential hazards, when in reality only a subset of these have been taken into account. Various protocols have been created to help structure this activity (see Table 1). Some approaches have defined enterprise risks according to their alignment with the degree of control that an organization has over mitigating the risk in question; Dey (2009) classifies these as business (external) risks and operational (internal) risks. Segmenting risks by division, department, and project levels, and grouping them according to whether they apply to individuals or the organization have also been considered (Reason, 2004). Unfortunately, these efforts have rarely yielded a complete set of risks that might impact the enterprise in part or as a whole (Holmes, 2002; Crouhy et al., 2006; Shenkir and Walker, 2010).

That the approaches attempted to identify enterprise risks may vary depending on the organization and its objectives is somewhat to be expected. As noted by Mikes and Kaplan (2014), each organization's independent approach to risk identification may be appropriate given their respective idiosyncrasies. In reviewing the information presented in Table 1, however, the approaches appear to vary more by differences in nomenclature than in the types of risks that might threaten an organization. This suggests that

TABLE 1
Risk Classifications

Author	Risk Categories	
Curtis and Concessi (2008)	* Regulatory	* Physical operations
	* Technical	* Volume
	* Price/market	* Modeling/valuation
	* Strategic	* Human capital
Miller and Waller (2003)	* Industrial uncertainties	* Firm-specific uncertainties
Dey (2009)	* Market	* Environmental and social
	* Financial	* Technological
	* Economical	* Political
Kaplan, Haimes, and Garrick (2001)	* Modal	* System
	* Information management	* User/stakeholders
	* Functional (subsystems)	* Management
	* Geographical/spatial	
Trammell, Lorenzo, and Davis (2004)	* Workers	* Customers
	* Community	* Company's physical assets
	* Environment	
U.S. Dept. of Transp. FHWA International Programs (2012) (Caltrans sample risk list)	* Technical	* Right-of-way
	* External	* Construction
	* Environmental	* Regulatory
	* Organizational	
U.S. Dept. of Transp. FHWA International Programs (2012) (WSDOT 2002 Urban Corridors Common Risks)	* Economic	* Geotechnical
	* Environmental	* Design process
	* Third party	* Construction
	* Right-of-way	* Other/minor
	* WSDOT Management	

an opportunity exists to develop a set of generic, yet more comprehensive enterprise risk categories that could be more widely accepted and utilized.

For each identified enterprise risk, the latter two steps of the risk triplet involve evaluating the respective likelihood of occurrence and the corresponding consequences should the event occur. Depending on the quality of data, available resources, and desired level of precision, organizations can opt to perform these steps using a more qualitative or quantitative technique. The qualitative approach tends to group event likelihood into terms that approximate gradations in frequency (e.g., extremely rare, rarely, occasionally, annually, often) and consequence (e.g., minimal, moderate, significant, severe, catastrophic). By contrast, a more quantitative assessment assigns distinct probabilities to event likelihood and characterizes consequences in monetary terms. This offers the added advantage of being able to quantify the “risk” of an event in dollars spent. It also

FIGURE 1**Recommended Enterprise Risk Categories**

- Financial management
- Information systems
- Weather-related and other natural systems
- Employee health & safety
- Human resources
- Supply chain
- Customer service
- Legal and political
- Infrastructure and equipment
- Reputational
- Environmental
- Security
- Operational
- Strategic

FIGURE 2**Initial RiskCatcher Risk Assessment Window****Select Risk Categories**

Which of the following risk categories apply to your organization that you would like to evaluate?

- ☐ Financial Management Risk
- ☐ Information Systems Risk
- ☐ Weather-Related and Other Natural Systems Risk
- ☐ Employee Health & Safety Risk
- ☐ Human Resources Risk
- ☐ Supply Chain Risk
- ☐ Customer Service Risk
- ☐ Legal and Political Risk
- ☐ Infrastructure and Equipment Risk
- ☐ Reputational Risk
- ☐ Environmental Risk
- ☐ Security Risk
- ☐ Operational Risk
- ☐ Strategic Risk

supports a more formal basis for evaluating risk reduction strategies, as a benefit/cost ratio can be derived, a precursor to determining whether the financial return on investment is sufficient justification to allocate the resources needed for strategy implementation.

Perhaps surprisingly, given the recent enthusiasm for establishing ERM as a core business practice, literature devoted to discussing ERM risk assessment protocols has been sparse (Hallowell et al., 2013). Only recently are publications beginning to address this

FIGURE 3

Prompt Following Selection of Employee Health and Safety Risk Category [Color figure can be viewed at wileyonlinelibrary.com]


















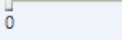
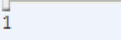
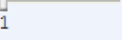





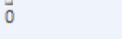
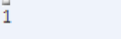
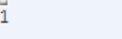




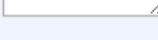



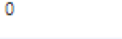
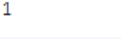
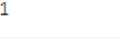
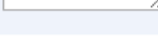
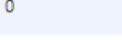
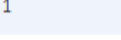
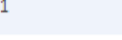
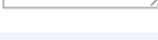
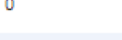
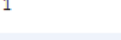
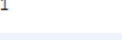
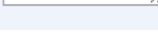
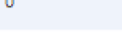
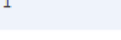
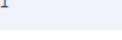
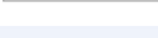



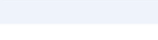
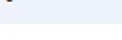
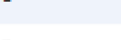
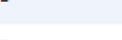




Risk Category	Risk Subcategory	Scenario Description	Frequency (0-6)	Property and Asset Consequences (1-6)	Human Health (injuries and fatalities) Consequences (1-6)
Employee Health & Safety Risk	Victim of assault or other criminal act				
Employee Health & Safety Risk	Subject to bullying or verbal abuse				
Employee Health & Safety Risk	Caught between, struck by physical object, or pinch points				
Employee Health & Safety Risk	Slips, trips, and falls				
Employee Health & Safety Risk	Fatigue				
Employee Health & Safety Risk	Uncomfortable ergonomics				
Employee Health & Safety Risk	Stress or mental anxiety				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Inhalation				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Ingestion				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Extreme hot or cold				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Loud noises				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Pungent odors				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Bloodborne pathogens				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Biological/bacterial hazards				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Fires and explosions				
Employee Health & Safety Risk	Exposure to harmful substances or environments - Carcinogens or radioactive materials				

FIGURE 4
Partial List of Corresponding Scenario Library

Victim of assault or other criminal act	Charges on company credit cards were for unauthorized purchases.
	Employees with company purchasing authority are victimized of identity theft by a group of cyber criminals.
	A company executive is accused of illegal business practices where someone has stolen his identity and used his information to commit crimes.
Subject to bullying or verbal abuse	A small group of employees appears to be picking on a younger, less experienced employee who is new to the organization.
	A group of employees begin verbally and physically abusing other employees.
Caught between, struck by physical object, or pinch points	Employee mashes finger in door jam or in equipment being used, resulting injury requiring medical treatment.
	Employee falls from a support structure to a lower level; or suffers serious burns to a portion of the body; or obtains cut due to an incident with a sharp object requiring stitches; or sustains a bone fracture due to an accident.
Slips, trips, and falls	Employee slips and falls due to liquids on the floor, unstable floor coverings, unstable support (e.g., chair, box, etc.) or weather conditions (e.g., ice, snow).
Fatigue	Employee makes mistakes with minor consequences in their normal job routine due to tiredness.
	One or more employees are found dozing off while on the job.
Uncomfortable ergonomics	Employees are required to perform routine tasks which can develop a debilitating condition (e.g., carpal tunnel).
Stress or mental anxiety	Job found to be very stressful and employee requires treatment by a psychologist, yet still able to perform their normal work load.
	Employee experiences anxiety attack and requires psychiatric treatment.
Inhalation exposure	Employee is exposed to moderately toxic vapors that are considered possible carcinogens, such as trichloroethylene.
Ingestion exposure	Employee is exposed to highly toxic vapors such as known carcinogens.
	Employee ingests fluid or debris while on the job that is moderately toxic.
Exposure to extreme hot or cold	Employee ingests fluid or debris while on the job that could result in death.
	Employee is exposed to hot materials (no direct contact with flames) when performing a directed task; or employee is dehydrated and shows signs of overexertion due to working on a hot summer day; or employee has debilitating symptoms due to exposure to winter weather conditions.
Noise exposure	Employee is routinely exposed to excessively loud noises and may suffer significant hearing loss.
Odor exposure	Employees are routinely exposed to extremely pungent odors and may become significantly ill.
Exposure to bloodborne pathogens, biological/bacterial hazards, carcinogens or radioactive materials	Employees required to deal with bloodborne pathogens are provided personal protective equipment (PPE), but do not always follow proper safety protocols when handling the materials or fail to use PPE.
	A large chemical or radiation release occurs in the facility and employees are exposed to high levels of toxicity before being evacuated/treated.
Exposure to fires and explosions	Employee is required to deal with fires or explosions on a regular basis or for an extended period of time. They are provided personal protective equipment (PPE), but do not always follow proper safety protocols when handling the materials or fail to use PPE.

consideration in the context of case studies (Altuntas et al., 2011; Arena et al., 2011) and related applications (Kaplan and Mikes, 2012; Pathak et al., 2013).

STRUCTURING AN ENTERPRISE RISK ASSESSMENT PROTOCOL

It was noted in the previous discussion that although there is a growing appreciation for the need to address risk management in an enterprise-wide, holistic, and integrated manner, the development of enterprise risk assessment techniques has not kept pace. Given that portions of enterprise risk are typically “owned” by different, mutually

FIGURE 5
 Scenario Likelihood and Consequence Rating Scale [Color figure can be viewed at wiley-onlinelibrary.com]

Frequency						
Level	1	2	3	4	5	6
	Extremely Rare	Rarely	Occasionally	Annually	Semi-annually	Frequently
Description	Occurrence interval		Occurrence interval	Occurrence interval	Occurrence interval	
	Occurs less than once in 25 years	between 10 and 20 years	between 5 and 10 years	between 1 and 5 years	between one month and one year.	Occurs at least once per month.
Consequence - Property/Asset Loss and Damage						
Level	1	2	3	4	5	6
	Minimal	Moderate	Significant	Moderately Severe	Extremely Severe	Catastrophic
Description	Between	Between	Between	Between	Between	
	\$0 and \$200	\$200 and \$2,000	\$2,000 and \$20,000	\$20,000 and \$200,000	\$2,000,000 and \$2,000,000	Greater than \$2,000,000
Consequence – Human Health						
Level	1	2	3	4	5	6
	Minimal	Moderate	Significant	Moderately Severe	Extremely Severe	Catastrophic
Description	Persons are treated on site for minor injuries and released, if any impact at all	Level 1 plus one or more persons requiring emergency room treatment	Level 2 plus one or more persons requiring hospitalization	Level 3 plus fatalities of 1 to 5 persons	Level 3 plus fatalities of more than 10 persons	Level 3 plus fatalities of more than 20 persons

exclusive parts of the organization, with little or no integration taking place, it is incumbent on a structured, holistic protocol to help organizations “get it right.” In the discussion to follow, an approach for satisfying this need is presented.

A proposed structure for categorizing enterprise risks is shown in Figure 1. Collectively, these categories cover a wide range of topics that should be of concern to an organization, while making it manageable for different parts of the organization to participate in the risk identification process based on their knowledge and expertise. It should be noted that the presence of a chief risk officer or another senior executive who owns the ERM responsibility is important in coordinating this effort and to ensure that any additional risks that involve interactions between these categories are recognized. For example, an off-site weather-related problem could inhibit the supply chain of a key material whose availability is time sensitive in supporting the organization’s production process.

The risk categories listed in Figure 1 are each separated into subcategories, and may be further disaggregated in order to classify the risk in an appropriate manner (see the Appendix). The category corresponding to weather-related and other natural systems risk, for example, contains the following risk subcategories: (1) atmospheric, (2) seismic, (3) geologic, and (4) hydrologic. The hydrologic subcategory is further segmented into:

1. coastal or river flooding
2. storm surge

FIGURE 6

Sample Qualitative Risk Assessment Results [Color figure can be viewed at wileyonlinelibrary.com]

Scenario Risk							
Risk Category	Subcategory/Scenario Description		Frequency	P&A Cons.	Health Cons.	Annual Event Occurrence	Annual Risk Score
Weather-Related and Other Natural Systems Risk	Atmospheric - Hurricane	Category 4 hurricane hits logistics operations center	1	5	2	0.04	0.28
Weather-Related and Other Natural Systems Risk	Atmospheric - Heavy rains	Heavy rains lead to minor flooding at terminal facility	4	2	1	0.33	1.00
Weather-Related and Other Natural Systems Risk	Hydrologic - Drought or desertification	Severe drought leaves water levels too low for inland navigation	2	5	1	0.07	0.40
Environmental Risk	Hazardous material release	Several hundred gallon oil spill results in contamination of waterway and shoreline	3	4	1	0.13	0.67
Operational Risk	Failure to follow procedures	Dock worker falls 20 feet to concrete floor due to failure to wear safety harness	2	1	5	0.07	0.40

Category Risk			
Category Title	Annual Number of Events	Total Consequence Score	Annual Risk Score
Weather-Related and Other Natural Systems Risk	0.44	7.04	3.10
Environmental Risk	0.13	0.67	0.09
Operational Risk	0.07	0.40	0.03

3. drought or desertification
4. salinization of groundwater
5. erosion and sedimentation

RISK CATCHER

In order to embrace the aforementioned risk identification format and provide for the ability to assign a likelihood and consequence to each identified risk to form a more complete enterprise risk assessment protocol, a web-based application was developed. The basis for this development effort was to create a product that could be widely available for organizations in the public and private sector to use, accessible at no cost. The availability of such a public domain tool would supersede the need for an organization to acquire an existing commercially available risk assessment software tool and/or retain a risk management consulting firm at significant expense.

The product of this effort, called RiskCatcher, is structured in a user-friendly, menu-driven format, with modules that mirror the previously described process steps.¹ It operates much in the same way as TurboTax[®], in that users select relevant risk categories, following which they are presented with selections within each category that are chosen to describe scenarios and corresponding scenario likelihoods and consequences. RiskCatcher can be used to perform both quantitative and qualitative risk assessments. Results are portrayed in graphic and tabular form, and may be exported to other software applications. The program also includes a library where relevant information can be sourced for use as default values to support various scenario evaluations. RiskCatcher can be accessed through the following URL: <http://transp40.vuse.vanderbilt.edu/riskcatcher/>.

¹ This article is being published with the understanding that *Risk Management and Insurance Review* is not endorsing the product.

FIGURE 7
 Sample Quantitative Risk Assessment Results [Color figure can be viewed at wileyonlinelibrary.com]

Scenario Risk

Risk Category	Subcategory/Scenario	Description	Frequency	P&A Cons.	Health Cons.	Annual Event Occurrence	Cons. per Event	Annual Cost
Financial Management Risk	Credit risk - Restricted access to credit	aaa	1	4	5	0.0	\$53,350,000	\$2,134,000
Financial Management Risk	Liquidity risk	bbb	2	2	2	0.1	\$251,100	\$16,740
Financial Management Risk	Recession/depression	ccc	2	5	2	0.1	\$1,150,000	\$76,667
Information Systems Risk	Software/Data – Infection (virus, malware, etc.)	ddd	5	2	5	6.0	\$52,261,000	\$627,132,000
Information Systems Risk	Hardware (PCs, laptops, PDAs, phones, etc.) - Upgrades (failure or lack thereof)	fff	6	1	2	12.0	\$50,100	\$601,200
Employee Health & Safety Risk	Subject to bullying or verbal abuse	ggg	2	4	4	0.1	\$52,360,000	\$3,490,667
Employee Health & Safety Risk	Fatigue	hhh	1	5	2	0.0	\$1,350,000	\$54,000
Employee Health & Safety Risk	Exposure to harmful substances or environments - Ingestion	jjj	6	6	6	12.0	\$85,450,000	\$1,025,400,000

Category Risk

Category Title	Annual Number of Events	Annual Risk Cost
Financial Management Risk	0.2	\$2,227,407
Information Systems Risk	18.0	\$627,733,200
Employee Health & Safety Risk	12.1	\$1,028,944,667

When RiskCatcher is accessed and the user has logged in, the user has the option of beginning a new qualitative or quantitative risk assessment or recalling a saved one. If a new risk assessment is selected, a menu of risk categories appears (see Figure 2). The user can select any number of these categories for further assessment. Depending on which boxes are checked, users receive a list of the subcategory options they may wish to consider. A link is also provided to a library of related scenarios to help the user further define the hazard in question. Figure 3 shows the screen when only the Environmental Health and Safety Risk category has been selected. Figure 4 displays a partial list of scenarios that could be associated with this category.

Note that in Figure 3, the user is also prompted to assign a frequency of occurrence as well as the corresponding consequence should the event occur. Consequences are divided in property/asset damage and human casualties, as we have found that users tend to treat these impacts in different dimensions.

The user is asked to provide a rating for frequency of occurrence and consequence using a sliding scale, according to the definitions provided in Figure 5. If the user previously selected a qualitative assessment, then the numerical entry into these cells is guided by the lightly shaded terminology. If a quantitative assessment is being performed, then the numerical descriptions in the table are utilized, and subsequently converted into probabilities and monetary impacts. Human casualties are assigned monetary values

based on the value of a statistical life and maximum abbreviated injury scale levels (Chatterjee and Abkowitz, 2011).

Figure 6 shows a completed RiskCatcher table for a sample qualitative risk assessment, while Figure 7 displays sample results for a quantitative risk assessment. Note that the results present an annual risk score and cost, respectively. This provides the user with insight as to which specific event scenarios pose the greatest threats to the enterprise. In the case of the quantitative results, an estimated annual cost of incurring this risk is provided, serving as a basis for determining the level of risk mitigation investment that may be appropriate.

Beyond these assessments at the event scenario level, risks can be rolled up into an overall assessment by risk category. These results also appear in Figures 6 and 7 for sample qualitative and quantitative assessments, respectively. A further roll-up can be performed to aggregate results at the enterprise level. Supporting graphs depicting these results are also provided as a user selection option.

RiskCatcher was successfully deployed in a pilot project involving a large marine carrier operating in the continental United States. Logical progression and ease of use were particularly noted during this exercise.

CONCLUDING REMARKS

In this article, we have reviewed the state of the practice of ERM, including tools that are available to support the enterprise risk assessment process. In doing so, it was observed that while recent trends are moving toward greater acceptance of ERM as an important business practice, a holistic, structured framework for assessing risks has yet to emerge. To overcome these limitations, we presented a conceptual approach for a new protocol and transformed it into a public domain, web-based tool. The tool is designed to be sufficiently flexible to conform to the unique risk portfolio that each organization encounters, while having the structure and containing the background information to enable its widespread use.

Like any other management guideline or decision-support tool, however, its usefulness is directly related to an organizational commitment to support an ERM initiative and to leverage what resources are available. In the case of ERM, conditions requiring organizations to be savvy about what can go wrong, the likelihood of occurrence and the potential impacts are only growing more complex and compelling. It is our hope that this work can help ease that process, enabling an enterprise to become less vulnerable and more resilient.

APPENDIX: RISK CATEGORIES

Financial Management

1. Credit risk
 - Restricted access to credit
 - Customer fails to make a payment
2. Liquidity risk
3. Financial forecasting error
4. Recession/depression

5. Currency exchange
 - Convertibility issues
 - Fluctuations in valuation
6. Unauthorized use of company funds
7. Money laundering

Information Systems

1. Software/data
 - Denial of usage
 - Infection (e.g., virus, malware)
 - Unauthorized access (e.g., piracy, leakage, alteration)
 - Lack of redundancy
 - Upgrades (failure or lack thereof)
2. Hardware
 - Denial of service/usage
 - Lack of redundancy
 - Theft/damage
 - Upgrades (failure or lack thereof)
3. Network
 - Unauthorized access
 - Insufficient bandwidth
 - Lack of redundancy
 - Upgrades (failure or lack thereof)
 - Abuse or misuse
4. Intellectual property
 - Copyright or domain theft
 - Unauthorized release of proprietary information (e.g., leakage, compromised devices)

Weather-Related and Other Natural Systems

1. Atmospheric
 - Hail
 - Hurricane
 - Lightning
 - Tornado
 - Heavy rains
 - Snow/ice
 - Strong winds
 - Sandstorm, wind erosion, or sedimentation
 - Heat wave
2. Seismic
 - Earthquake
 - Tsunami
 - Seiche

3. Geologic
 - Avalanche
 - Volcano
 - Expansive soil
 - Sinkhole
 - Landslide/mudslide
 - Rock fall
 - Subsidence
4. Hydrologic
 - Coastal or river flooding
 - Storm surge
 - Drought or desertification
 - Salinization of groundwater
 - Erosion and sedimentation

Employee Health and Safety

1. Victim of assault or other criminal act
2. Subject to bullying or verbal abuse
3. Caught between, struck by physical object or pinch points
4. Slips, trips, and falls
5. Fatigue
6. Uncomfortable ergonomics
7. Stress or mental anxiety
8. Exposure to harmful substances or environments
 - Inhalation
 - Ingestion
 - Extreme heat or cold
 - Loud noises
 - Pungent odors
 - Blood borne pathogens
 - Biological/bacterial hazards
 - Fires and explosions
 - Carcinogens or radioactive materials

Human Resources

1. Insufficient compensation and/or benefits
2. Low morale
3. Disgruntled or angry employee behavior
4. Inadequate training
5. Employee participation in illicit activities
 - Addictions

- Domestic violence
 - Other
6. Transient/unreliable labor pool

Supply Chain

1. Product/material/transportation cost increases and uncertainties
2. Lengthy and variable transportation and loading/unloading times
3. Improper forecasting of supply/demand
4. Supplier delivery failure
 - Late or nondelivery of ordered product/material
 - Receipt of damaged or wrong product/material
 - Receipt or use of products/materials with safety hazards
5. Loss of supplier
 - Out of business
 - Opts to serve other customers instead
 - Contract impasse
6. Transportation infrastructure failure
7. Lack of fuel availability

Customer Service

1. Being dishonest or unfair with customer
2. Harsh, careless, disrespectful, or impersonal treatment of customer
3. Employees lacking a desire, capability, or authority to solve problems
4. Being inaccessible to customer when concerns arise
5. Poor record keeping
6. Lack of timely response
7. Failing to deliver promised products or services
8. Inadequate communication after problems arise

Legal and Political

1. Organization specific
 - Failing to meet regulations or facility ordinances
 - Confiscation of equipment
 - Expropriation of company
 - Labor strike
 - Breach of contract
 - Sabotage
 - Kidnapping, extortion, or theft
 - Boycott within organization

2. Macro-level

- Mass nationalizations
- Regulatory changes
- Changes in tort liability judgments/awards
- Mass labor strikes
- Rioting
- Censorship and privacy
- Civil war
- Import/export trading imbalances
- Illicit trade activity (black market)
- Scarcity of water, food, or energy
- Pandemic
- Nuclear attack/disaster
- Social unrest

Infrastructure and Equipment

1. Design, construction, or installation defect/error/omission
2. Mechanical breakdown
3. Destruction or loss of property due to theft, unauthorized transfer, or vandalism
4. Exposure to insects, birds, or other animals
5. Weathering/contamination of equipment/infrastructure, including fungus, wet/dry rot, or exposure to extreme heat/cold
6. Fire, implosion, or explosion
7. Facility water line leak
8. Power failure
9. Water source failure
10. Improperly secured objects
11. Random incident

Reputational

1. Unfair labor and trade practices
2. Lack of corporate social responsibility
3. Lack of philanthropy
4. Disrespect for human rights
5. Failing to follow the rule of law
6. Corruption
7. Employee participating in illicit activities
8. Abuse of indigenous rights

9. Endangerment to public health
10. Lack of environmental and community stewardship
11. Generic reputation issues

Environmental

1. Pollution
 - Air
 - Water
 - Land
 - Noise
 - Odor
2. Introduction of invasive species
3. Habitat destruction
4. Soil erosion
5. Hazardous material release

Security

1. Terrorism
 - General
 - Gang violence
 - Use of weapons of mass destruction
2. Drug trafficking
 - Cargo
 - Employee
3. Abuses by security personnel
4. Vandalism
5. Kidnapping
6. Corporate espionage

Operational

- Lack of quality control
- Operating inefficiency
- Improper, failed, or lack of communication
- Failure to follow procedures

Strategic

1. Weak corporate governance
 - Lack of leadership, management oversight
 - Arrogance

- Institutional inertia
 - Imposition of unreasonable economic and scheduling expectation
 - Lack of planning and preparedness
2. Market risk
 3. Merger and acquisition risk
 4. Lack of diversity in customer base
 5. Vulnerable to emerging technologies
 6. Pool talent management—retention or succession planning
 7. Outpaced by competition

REFERENCES

- Accenture, 2011, Global Risk Management Study.
- Ai, J., P. L. Brockett, W. W. Cooper, and L. L. Golden, 2012, Enterprise Risk Management Through Strategic Allocation of Capital, *Journal of Risk and Insurance*, 79(1): 29-56.
- Altuntas, M., T. R. Berry-Stölzle, and R. E. Hoyt, 2011, Implementation of Enterprise Risk Management: Evidence From the German Property-Liability Insurance Industry, *Geneva Papers on Risk & Insurance*, 36(3): 414-439.
- Arena, M., M. Arnaboldi, and G. Azzone, 2011, Is Enterprise Risk Management Real? *Journal of Risk Research*, 14(7): 779-797.
- Australian/New Zealand Standard, 2004, Risk Management, 4360: 2004.
- Chatterjee, S., and M. Abkowitz, 2011, A Methodology for Modeling Regional Terrorism Risk, *Risk Analysis*, 31(7): 1133-1140.
- Committee of Sponsoring Organizations of the Treadway Commission, 2004, Enterprise Risk Management—Integrated Framework.
- 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, and R. Mark, 2006, *The Essentials of Risk Management* (New York: McGraw-Hill).
- Curtis, P. C., and P. Concessi, 2008, The Risk Intelligent Energy Company: Weathering the Storm of Climate Change, *Oil and Gas Financial Journal*, 51(1): 1-4.
- Dey, P., 2009, Managing Risks of Large Scale Construction Projects, *Cost Engineering*, 51(6): 23-27.
- Gates, S., and E. Hexter, 2005, From Risk Management to Risk Strategy. The Conference Board Inc.
- Hallowell, M., K. Molenaar, and B. Fortunato, 2013, Enterprise Risk Management Strategies for State Departments of Transportation, *Journal of Management in Engineering*, 29(2): 114-121.
- Health Service Executive, 2009, Developing and Populating a Risk Register: Best Practice Guidance.

- Holmes, A., 2002, *Risk Management* (Oxford, UK: Campstone Publishing).
- Hoyt, R. E., and A. P. Liebenberg, 2011, The Value of Enterprise Risk Management, *Journal of Risk and Insurance*, 78: 795-822.
- International Organization for Standardization, 2009, Risk Management—Principles and Guidelines, ISO 31000:2009, Geneva, Switzerland.
- Kaplan, R. S., and A. Mikes, 2012, Managing Risks: A New Framework, *Harvard Business Review*, 90(6).
- Kaplan, S., Y. Y. Haimes, and B. J. Garrick, 2001, Fitting Hierarchical Holographic Modeling (HHM) Into the Theory of Scenario Structuring, and a Refinement to the Quantitative Definition of Risk, *Risk Analysis*, 21(5): 807-819.
- Kennedy, D., 2005, Risks and Risks, *Science*, 309(5744): 2137.
- Kleffner, A. E., R. B. Lee, and B. McGannon, 2003, The Effect of Corporate Governance on the Use of Enterprise Risk Management: Evidence From Canada, *Risk Management and Insurance Review*, 6: 53-73.
- Liebenberg, A. P., and R. E. Hoyt, 2003, The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers, *Risk Management and Insurance Review*, 6(1): 37-52.
- Mikes, A., and R. Kaplan, 2014, Towards a Contingency Theory of Enterprise Risk Management, Working Paper, Harvard Business School, 13(063).
- Miller, K., 1992, A Framework for Integrated Risk Management in International Business, *Journal of International Business Studies*, 23: 311-332.
- Miller, K. D., and H. G. Waller, 2003, Scenarios, Real Options and Integrated Risk Management, *Long Range Planning*, 36(1): 93-107.
- Nocco, B. W., and R. M. Stulz, 2006, Enterprise Risk Management: Theory and Practice, *Journal of Applied Corporate Finance*, 18(4): 8-20.
- 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.
- Oryang, D., 2002, *Probabilistic Scenario Analysis (PSA)—A Methodology for Quantitative Risk Assessment* (Puerto Vallarta, Mexico: NAPPO PRA Symposium).
- Pagach, D., and R. Warr, 2011, The Characteristics of Firms That Hire Chief Risk Officers, *Journal of Risk and Insurance*, 78: 185-211.
- Pathak, J., E. K. Khondkar, C. Carter, and Y. Xie, 2013, Why Do Enterprise Risk Management Systems Fail? Evidence From a Case Study of AIG, *International Journal of Applied Decision Sciences*, 6(4): 345-371.
- Reason, J., 2004, Managing the Risks of Organizational Accidents. Presented at RMC V, Cleveland, OH. World Wide Web: http://rmc.nasa.gov/archive/rmc_v/presentations/reason%20managing%20the%20risks%20of%20organizational%20accidents.pdf (accessed March 2014).
- Shenkir, W. G., and P. L. Walker, 2010, Enterprise Risk Management, Accounting Policy and Practice Series, Bureau of National Affairs—Tax and Accounting Portfolio 5303.
- Smithson, C., and P. Song, 2004, Quantifying Operational Risk, *Risk*, 17:50-52.

- Togok, S. H., and S. Zainuddin, 2014, Review of Enterprise Risk Management (ERM) Literature, Proceedings of the International Conference on Technology and Business Management, Dubai, pp. 36-48.
- Trammell, S. R., D. K. Lorenzo, and B. J. Davis, 2004, Integrated Hazards Analysis, *Professional Safety*, 49(5): 29-37.
- U.S. Department of Transportation, Federal Highway Administration, 2012, Transportation Risk Management: International Practices for Program Development and Project Delivery, Report No. FHWA-PL-12-029.