RISKY BUSINESS: MAXIMIZING PERFORMANCE BY EFFECTIVELY MANAGING ON THE RISK-CRISIS FRONTIER

There may be substantial gains to be had by integrating ERM and crisis management to get one cohesive set of tools that allows an organization to take on risks that promise to return more benefit than cost.

CJ MCNAIR-CONNOLLY, GREG WALLIG, AND LAUREN PASHIA

Risk management is a well-developed field where key concepts have been defined and explored in a variety of contexts. When risk mitigation fails, though, an organization often faces a crisis. Less has been written about crisis management, with the dominant themes in the literature being leadership and communication in crisis situations. Since risk and crisis management are so closely related, there is significant benefit to be achieved by integrating the two fields into one set of diagnostics and management tools. The goal of the Integrated Risk and Crisis Management (IRCM) interest group at CAM-I is to explore this integration, modifying existing thought and practice to enable organizations to maximize their risk position while actively managing on the edge of the risk-crisis frontier.

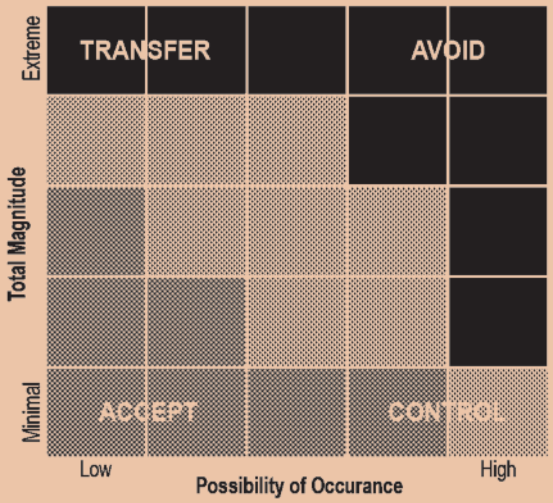
To be in business is to face a constant stream of potential risks that can disrupt daily activity and put the future of the organization in jeopardy. Risk, or the

CJ MCNAIR-CONNOLLY *is an internationally recognized expert in cost management. She has authored ten trade books and numerous articles on various aspects of the relationship and development of cost management and the new technologies that define modern management practice. Holding an MBA and Ph.D. from Columbia University, Dr. McNair-Connolly is a retired professor of accounting from the U.S. Coast Guard Academy. She has been active in various research projects with CAM-I since 1986.*

GREG WALLIG, CISA, CGEIT, *is the managing director of Grant Thornton. With over 20 years' consulting experience in both the public and private sectors, Greg brings a diverse perspective to organizations that are seeking to optimize the performance of their business. Greg leads Grant Thornton's Global Public Sector governance, risk, and compliance and information assurance practices. Greg focuses on enterprise risk management, information assurance, program integrity, internal controls and forensic accounting. He frequently writes and speaks on the topic of utilizing risk management concepts to improve the efficiency and effectiveness of government programs. He has been with CAM-I for one year.*

LAUREN PASHIA *is an integrated scheduler with The Boeing Company, supporting the Phantom Works Research & Development business unit. Lauren's expertise includes scheduling and financial operations and analysis. Lauren holds both a bachelor's and master's degree in business administration. She has been active with CAM-I for just less than one year, joining the IRCM interest group at a critical time and making major contributions to the project.*

EXHIBIT 1 Example of a Heat Map

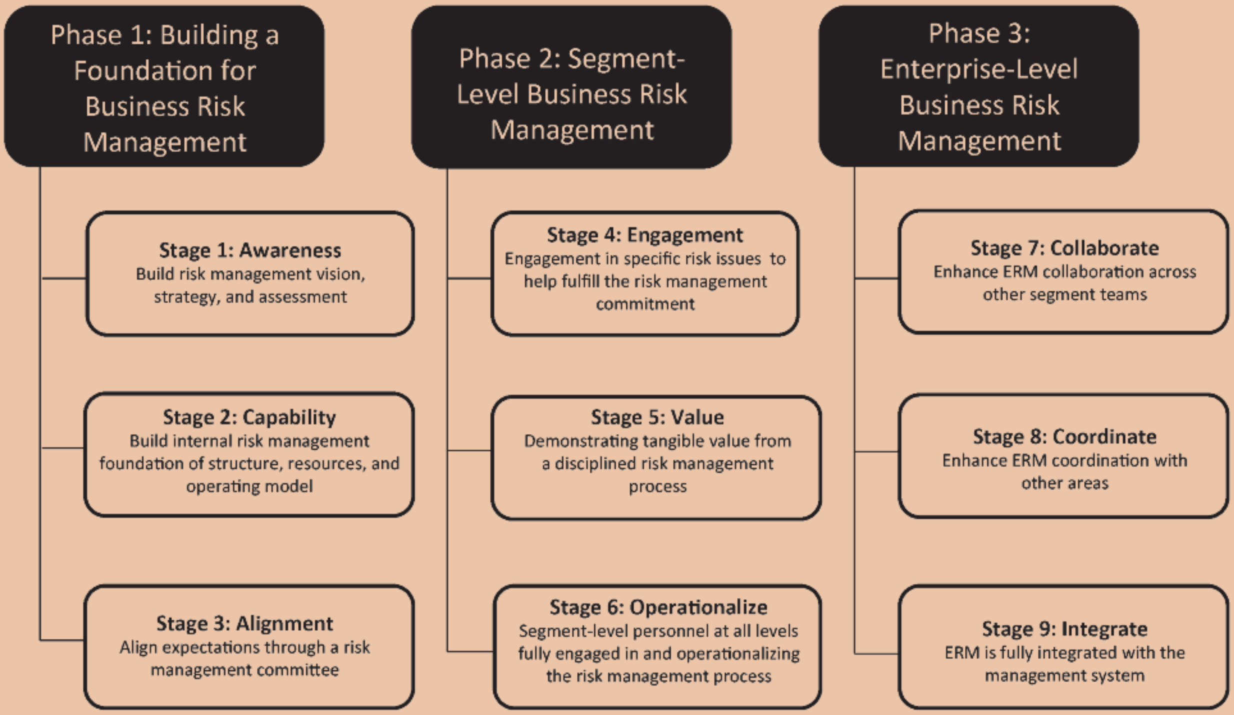


probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, can be mitigated to some extent through preemptive action.[1] While some risks may actually be exploited to yield positive results, risk remains a disruptive event in an organization's life. Therefore, risk can be seen as an entity's intentional interaction with uncertainty. Finding ways to mitigate risk is the entire focus of the discipline of enterprise risk management (ERM). When a risk cannot be mitigated, or the mitigation attempts are inadequate, the organization can face a crisis situation. Crisis or a change, sudden or evolving, results in an urgent problem that must be addressed immediately, as it has the potential to greatly damage an organization's reputation, finances, operations, and people, and destroy the trust it has established with its stakeholders.[2]

To date, there is little or no overlap in the literatures on and practices of ERM and crisis management. Although the two fields are tightly tied together by nature, forming a continuum of risky business settings, the ERM literature has emphasized mitigation strategies and techniques, while the crisis literature has placed its priorities on the issues of leadership and communication during crisis conditions. It would seem logical that these two disciplines should be linked, allowing for a smooth transition between risk and crisis management. Even more important is the fact that organizations may be able to learn how to operate effectively by taking on measured risks that boost returns to stakeholders. The goal should not be to avoid all risks, but rather to have a functioning risk management approach that seeks to optimize risk-taking by helping the organization operate at the point where risk is exploited to extract the most enterprise value out of its current offerings of products and services in a way that its competition cannot.

In this article, we briefly review the ERM and crisis management literatures, and then suggest that there may be substantial gains to be had by integrating the two disciplines to get one cohesive set of tools that allows an organization to take on risks that promise to return more than cost. As a first phase in this effort to integrate risk and crisis management, we'll suggest a revised model of the traditional risk heat map that emphasizes the zones where plans need to be made to prevent or curb the destructiveness of a crisis. This new perspective opens up the field for discussion regarding how best to integrate risk and crisis management

EXHIBIT 2 IMA's ERM Maturity Model


Phase 1: Building a Foundation for Business Risk Management
Stage 1: Awareness
Build risk management vision, strategy, and assessment
Stage 2: Capability
Build internal risk management foundation of structure, resources, and operating model
Stage 3: Alignment
Align expectations through a risk management committee
Phase 2: Segment-Level Business Risk Management
Stage 4: Engagement
Engagement in specific risk issues to help fulfill the risk management commitment
Stage 5: Value
Demonstrating tangible value from a disciplined risk management process
Stage 6: Operationalize
Segment-level personnel at all levels fully engaged in and operationalizing the risk management process
Phase 3: Enterprise-Level Business Risk Management
Stage 7: Collaborate
Enhance ERM collaboration across other segment teams
Stage 8: Coordinate
Enhance ERM coordination with other areas
Stage 9: Integrate
ERM is fully integrated with the management system

tools to get metrics and models that keep an organization in the zone of effective risk-taking and optimized performance. Let's start the discussion by detailing the existing state of the art.

Enterprise risk management: Searching for mitigation strategies

ERM is concerned with both the risks and opportunities that affect the value creation processes or impact organizational sustainability. It has been defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the following way:

> *Enterprise Risk Management* (ERM) is a process, effected by an entity's board of directors, management, and other personnel, applied in a strategic setting and across the enterprise, designed to identify and manage risks to stay within the risks appetite-tolerance level of the organization, in order to provide reasonable assurance that entity goals and objectives will be achieved.[3]

While this definition stresses the strategic nature of ERM, in reality, risks can occur at the strategic, tactical, and operational levels of the organization. And, not all risks are negative. There are many situations that arise where a sudden event offers the organization a chance to make substantial competitive gains. In ERM, though, the predominant attitude is one of finding ways to avoid risks wherever possible.

The response to identified risks in the organization is based on their perceived severity and includes controlling, avoiding, accepting, or transferring the risk to an external party. Insurance is one way that risk is transferred to another organization. As can be seen by these potential responses, risk management is an active exercise that takes place whenever and wherever an organization undertakes the assessment of current operations and future opportunities for growth. In dealing with risk, then, ERM emphasizes the organization's risk appetite, or the amount of risk the organization's management is willing to take at any given moment in pursuit of value. It reflects the

EXHIBIT 3 Crises Defined by Cause

Economic Related

- Labor problems, stock market crash, hostile takeovers, changes in trade policy, sharp decline in earnings, loss of major customer account

Informational

- Tampering with computer records, Y2K, loss of proprietary and confidential information

Physical

- Loss of key equipment or materials, breakdown of key equipment, explosion, faulty product design, product failures

Reputational

- Slander, gossip, rumors, damage to corporate reputation

Psychopathic Act

- Product tampering, kidnapping terrorism, workplace violence

Natural Disasters

- Earthquakes, fires, floods, hurricanes, tornadoes

Human Resource

- Loss of key personnel or executive, rise in workplace accidents, sexual harrassment, decline in employee morale, strikes

entity's risk management philosophy and, in turn, influences the entity's culture and operating style. Risk appetite guides resource allocation, assists the organization in aligning its structure, people, and processes in designing the infrastructure necessary to effectively respond to and monitor risks.

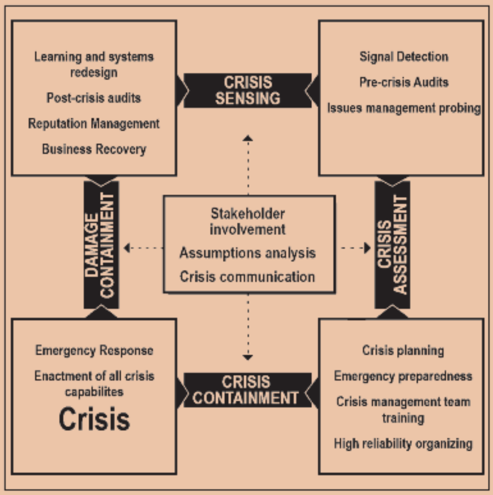
Risk tolerance captures a larger zone where, for some outcomes, the organization is willing to take on an additional increment of risk because the promised payoff is significant. It is the acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives. For instance, when retirement portfolio risk is considered, an individual may only be willing to tolerate a five percent variation in returns. This is this individual's investment risk tolerance.

There is inherent risk in almost any undertaking — by definition, the organization is taking a chance when it takes action to improve its competitive position. Inaction, either intentional or unintentional, may impact inherent risk, as risk is measured relative to the organization's operating environment and objectives and therefore is not static. Mitigation strategies help to bring this risk into the risk tolerance zone, but there is always a residual amount of risk left after mitigation has taken place. There are four core concepts involved in a risk: frequency, severity, correlation, and uncertainty. There are tools that place a risk somewhere along the continuum of frequency and severity, classifying the risks that management needs to pay attention to. The modified heat map, developed by the IRCM interest group and presented in Exhibit 1, is one such tool. When risk and crisis management are integrated, the red zone where crisis management plans are developed in depth is extended to include low probability, high impact events. This is a lesson learned from the effort to integrate the two disciplines.

COSO is one of the leading sources of information on internal control and ERM. This organization recently published a revised comprehensive guide to enterprise risk management called *Internal Control: Integrated Framework*. Arising from the financial crisis of 1996, COSO seeks to provide guidance on how organizations can recognize and manage risks. One of the most notable outcomes of the COSO report is the COSO cube, which categorizes risks on three dimensions: type of risk (operational, reporting, compliance), the efforts taken to manage risks (control environment, risk assessment, control activities, information and communication, and monitoring activities), and the level of the organization facing the risks (entity, division, operating unit, or function).

There are many models and methods of depicting the maturity of an ERM system inside an organization. One of the most informative has been developed by the Institute of Management Accountants in 2007. A version of this diagram is presented in Exhibit 2.[4] Here, we see organizations developing capabilities with respect to risk management as a continuum of expertise. This expertise is built by exercising more active management and communication of risk activities throughout the organization. Having briefly reviewed the state of the art in ERM, let's now turn our attention to the discussions around crisis management that define the current state of the art.

EXHIBIT 4 A Systems View of Crisis Management



From risk to crisis

There are four elements common to most definitions of crisis:

1. a threat to the organization, such as loss of life, environmental disaster, loss of key customers, or competitive threats that could invalidate the organization's core strategy;
2. the element of surprise;
3 a critical decision time frame; and
4. the potential for significant damage to either the organization's financial, operational, or reputational state.

A crisis is very different from a problem. A problem is something that takes place frequently and for which coping devices have been developed. Taking an airline as an example, weather delays and maintenance problems are practically a daily event for airlines that cross nations and oceans. On the other hand, airline crashes are infrequent and highly charged events in which the airline is forced to make rapid decisions with inadequate information; the airline is on the spot to deliver timely updates to the public from the moment the crisis occurs.

A problem, then, is frequent, affects few stakeholders, and has mostly an internal focus. A crisis on the other hand is significant, rare, affects multiple stakeholders, and requires both an internal and external focus. There are two main categories of crises: sudden and smoldering. Sudden crises are events such as airplane crashes, which happen suddenly and require a rapid response. Smoldering crises reflect management problems; small problems are not given attention, so they snowball into large problems that place the organization and its survival at risk. A smoldering crisis, then, evolves over time — precious time — during which management can take strategic moves to mitigate the potential crisis. When people think of crises, they tend to visualize sudden and acute events like hurricanes and tsunamis, not the impact of changing regulatory structures on an industry's competitive positioning.

The causes of a crisis are varied, as suggested by Exhibit 3.[5] As the list suggests, there are many causes of a crisis, ranging from the basic economics of the organization to natural disasters. What all of these crises have in common is that they put the organization in jeopardy; a poorly managed crisis can destroy an organization.

An example of a recent major crisis was the Fukushima Daiichi incident where the nuclear reactor's tsunami wall was

EXHIBIT 5 The Integrated Risk and Crisis Management Special Interest Group Details

Origination Date: March 2013

Key Members: Boeing, Grant Thornton, Vion Corp., Dresser-Rand, United States Coast Guard, Navistar, U.S. Army, DuPage College

Current Output: White paper on Integrated Risk-Crisis Meter, formula for risk-crisis metric

Future Deliverables: Maturity model for IRCM, scoring templates, metric for placing organization on risk-crisis frontier

breached, pouring millions of gallons of water into the system, resulting in the release of radioactive gases into the surrounding atmosphere. Back-up generators needed to keep the plant from melting down were swamped by the tsunami's 13-meter wave. The resulting loss of power, which was mitigated by a battery back-up that lasted only one day, resulted in a category seven radioactive disaster. Only Chernobyl had been given this rating in the past. This was a hazard risk, one that can be planned for but never avoided. Management had built a 10-meter wall to protect the facility, but this was breached by the 13-meter tsunami wave. Mitigation efforts were unsuccessful, as can often be the case. If management had taken the time to assess whether or not 10 meters of wall were adequate, perhaps they would have taken the initiative to build the wall higher. The point is clear — not all mitigation strategies are successful.

Crises, then, are unavoidable facts of organizational life. No organization is immune to crises and, in fact, it has been found that once one crisis strikes an organization, other crises follow quickly on its heels. There is a snowball effect with crises. Organizations need to prepare, in advance, for crisis events. If organizations have effective key risk indicators (KRIs, or measurements that are an indicator of the possibility of future adverse impact) in place they may be able to stop a crisis in its tracks in its prodromal, or pre-event, stage. KRIs give an organization early warning signals that identify potential events that may harm the continuity of the organization. When stopped in the prodromal stage, the crisis does not evolve into a disruptive event. KRIs are useful monitoring tools that help organizations detect, manage, or avoid crisis events.

Once a crisis has passed from its prodromal stage, it becomes acute. In other words, the crisis is now actually causing disruption and damage to the organization. Damage is done to the organization's sustainability and competitiveness once this stage is reached. In the acute stage of a crisis, management must become highly visible and in constant communication, providing honest, reliable answers to the voiced concerns of the organization's stakeholders. This essential, timely response is the reason why crisis management literature stresses leadership and communication as the key skills for an organization to have during a crisis event.

In October of 1982, Johnson & Johnson faced an enormous crisis when seven people in Chicago were reported dead after taking extra-strength Tylenol capsules. An unknown suspect put 65 milligrams of deadly cyanide into Tylenol capsules, 10,000 times more than is necessary to kill a human. The tampering did not take place in the Johnson & Johnson factories, but instead occurred once the product had been placed on store shelves. Johnson & Johnson immediately removed all Tylenol products from store shelves, but even with this aggressive and costly response, the company saw its market share and profits plummet. By taking responsibility for the problem and putting public safety first, though, Johnson & Johnson was able to regain customers' trust using aggressive marketing and public relations campaigns. The organization took effective actions in the acute stage, minimizing the effect the potential crisis had on the firm's reputation and financial position.

Not all companies react so effectively to an acute crisis. Some try to ignore the crisis, hoping it will resolve itself on its own. In this case, the crisis becomes chronic, eating slowly away at the firm's reputational and financial assets. The crisis at Arthur Andersen was one such event. Management tried to ignore the problems it was having in the areas of professional conflicts between their audit and consulting businesses, ultimately bringing the firm down when it became involved in the Enron scandal. Many product recall crises also fall into this chronic stage, as witnessed in the ongoing recall of Toyota automobiles over the past few years. When a crisis becomes chronic, it is very difficult to manage it effectively.

Crisis management is the set of tools and techniques that has been developed to help an organization handle a crisis when it occurs. There are five stages common to the handling of most crises: signal detection (the prodromal stage), when organizations that are capable crisis managers detect the early warning signs given by their KRIs of a potential crisis; preparation/prevention, where plans and policies are put in place to deal with a crisis; containment/damage control, where efforts are made to limit the reputational, financial, and other threats to the organization with rapid decision-making, the key to success; business recovery, where plans are made to return the organization to normal operations; and learning, where the lessons learned during the crisis are analyzed and communicated throughout the organization.[6]

NYU Hospital learned that it did not effectively mitigate the risks caused by flooding from a hurricane. Hurricane Sandy resulted in a loss of power that sent the hospital staff scrambling to care for affected patients. While it had moved the fuel supplies to run the hospital's generators out of danger, it had not moved the electrical panel that controlled the switchover to generator power. The result was a power loss that disrupted operations for a significant period of time. NYU Hospital has now taken steps to ensure that future flooding will not affect the organization's ability to serve the public.

Aspaslen and Mitroff take a systems approach to crisis management, as suggested by Exhibit 4.[7] In this model, learning occurs after the damage containment stage. What is interesting about this model is that it places emphasis on pre-crisis audits. The goal in this setting is to enable management to envision as many potential crises as possible. During the vulnerabilities audit, leadership should include managers from throughout the organization getting everyone ready to respond to a crisis. This diagram provides a concrete, tactical tool for an organization to use when it is planning for and responding to crisis events.

Part of preparing for a crisis is developing a crisis management plan that includes the role of communication in keeping stakeholders apprised of current conditions. Disaster drills done by local authorities are one such type of preparation plan. Here, individuals practice the skills they'll need if a crisis does occur. It's important to have trained communication specialists to handle the media and other stakeholders' inquiries to ensure that the organization puts the best foot forward in the event of a crisis. What you don't want is something like BP Oil's president's response that he "just wanted to get his life back" after the massive BP oil spill in the Gulf of Mexico in 2010. This communication failed to put the parties affected by the crisis at ease — it instead inflamed an already precarious situation for the organization. As this example suggests, communicators need to be trained to ensure only the most reliable and useful information is put in front of stakeholders.

PART OF PREPARING FOR A CRISIS IS DEVELOPING A CRISIS MANAGEMENT PLAN THAT INCLUDES THE ROLE OF COMMUNICATION IN KEEPING STAKEHOLDERS APPRISED OF CURRENT CONDITIONS.

Integrating risk and crisis management

Crises occur even when risks are mitigated. This means that risk and crisis management disciplines are linked by nature. The key linkage between the two disciplines is their scope: the crisis vulnerability audit is a simple extension of the risk audit. The goal in both disciplines is for early identification of a risk that may turn into a crisis, and the development of effective plans to mitigate the impact of the realized risk. As determined by the IRCM, there are a number of steps that organizations can take to integrate their risk and crisis management efforts, including the following.

- Pay attention to, identify, collect, and manage the risks. With integrated management of the two disciplines as the focus, risk mitigation and crisis planning become one event.

- Classify the potential impact and probability for each risk identified and develop crisis plans for those risks deemed likely or most damaging to the organization's survival.
- Assemble data that supports both risk and crisis management activities, with a team set up to integrate the information so that both efforts are using the same information and playbook.
- Coordinate the weighted approach to risk factors so that both initiatives are working from the same set of priorities.
- Develop a scorecard system that is used by both efforts, such as a heat chart.
- Develop mitigation plans that emphasize the rapid and effective resolution of a crisis once it occurs.
- Query all risks to identify those that, if they occur, will cause major damage to the organization's financial, operational, or reputational assets.
- Use metrics such as KRIs to constantly scan the environment for situations where risks may be realized so they can be effectively mitigated in the prodromal stage.
- Develop proactive communication plans, including communication trees that will enable the organization to respond quickly to crisis events. Also contact key stakeholders using methods that were developed prior to the crisis event. These actions should be part of the mitigation strategy.
- Try to integrate the communication system so that one message can be sent to all suppliers and key customers. Elements of the communication system should include the use of websites and toll free numbers to open all channels of communication to stakeholders. This approach should once again be considered part of the risk mitigation strategy.
- Learn from the crisis events so that better mitigation strategies can be put in place in the future.

There is more to be learned from integrating risk and crisis management, however. By learning where the boundaries are between a risk and a crisis event, management can effectively accept risks up to the point where crisis situations may loom. Knowing how much risk can be tolerated is more than a gut feeling. It can be measured using tools that include KRIs and a defined list of the contributing factors for each potential crisis event.

BY LEARNING WHERE THE BOUNDARIES ARE BETWEEN A RISK AND A CRISIS EVENT, MANAGEMENT CAN EFFECTIVELY ACCEPT RISKS UP TO THE POINT WHERE CRISIS SITUATIONS MAY LOOM.

The path forward

Having visualized the relationship between risk and crisis management, attention now needs to turn to developing a practical approach that an organization can implement to help monitor where it is on the risk-crisis continuum. The desired result is one integrated measure that includes the risk factors, contributing factors, and risk tolerance of the organization (one metric that details whether the organization is properly positioned with respect to risk-taking or whether it needs to increase or decrease its risk-taking activities). The IRCM interest group is actively working on the development of a practical formula and measurement approach that will tell an organization where it currently resides on the risk-crisis continuum. Exhibit 5 provides more information on the group.

One of the lessons learned from this exercise is that smoldering risks are different than acute risks in many ways. When an organization is operating under smoldering crisis conditions, there are multiple signals received that a crisis is imminent if effective management steps are not taken. For a smoldering crisis, there is time for management to gather, integrate, and respond to the KRIs and key performance indicators that serve as signaling devices.

In an acute crisis, there really isn't time to query potential responses and make minor adjustments; the organization has to go into crisis response mode and make rapid decisions about how best to reduce the impact of the crisis on stakeholders and the organization's survival potential. In the case of an acute crisis, the smoldering crisis condition all but disappears on the risk-crisis continuum; a flashpoint is passed very quickly.

Future efforts by the IRCM interest group include the development of a set of business cases that illustrate how various organizations have effectively dealt with both smoldering and acute crises. The team will also specifically define the metric used to measure where an organization is on the risk-crisis continuum. In the process of defining this metric, the team will develop a scoring template for risk tolerance as well as a scoring template for impact/likelihood of the crisis. A maturity model for risk-crisis management will be developed that helps an organization understand its strengths and opportunities for growth in this vital area. Included in this maturity model will be a sample risk-crisis management plan for organizations that find themselves in the smoldering crisis condition. In total, the group's efforts will be to knit together the two disciplines to provide an integrated approach to risk and crisis management that can be used by organizations to maximize the returns they earn for the risks they take. ■

NOTES

[1] "Risk," Business Dictionary. Available at: http://www.businessdictionary.com/definition/risk.html.

[2] *Managing Crisis*. (Boston: Harvard Business Press Pocket Mentor, 2008): 4; Examples of types of risks that could potentially be exacerbated in the event of a crisis (an asterisk indicates an external event) include: strategic (loss of reputation (external)*, loss of reputation (internal), decline in core demand*, competitor infringement on core market*, M&A benefits not delivered, competitive price wars*, senior management turnover, failure to expand alternative revenue sources, loss of key customer*, supplier problems*), operational (cost overruns, management ineffectiveness, technological failures, personnel retention, poor quality, cyber security threats*), compliance (regulatory (SEC, FCPA, OSHA), failure to recognize/meet changing regulations, privacy requirements, OSHA requirements, loss of intellectual property, HR-related requirements, protecting intellectual property), financial (excessive financial leverage, margin pressure*, financial restatements, accounting irregularities, fraud), and hazard (lawsuits*, natural disasters*, pandemics*, terrorist acts*, government shut-down*).

[3] COSO *Enterprise Risk Management—Integrated Framework*, Executive Summary (Sept 2004): 2.

[4] Exhibit 2 is based on *Enterprise Risk Management: Tools and Techniques for Effective Implementation*. (Montvale, NJ: Institute of Management Accountants, 2007).

[5] Exhibit 3 is based on James, E. and Wooten, L., *Leading Under Pressure: From Surviving to Thriving Before, During, and After a Crisis*. (New York: Routledge, 2010): 25.

[6] *Ibid*.

[7] Exhibit 4 is based on Aspaslen, C. and Mitroff, I., *Swans, Swines and Swindlers: Coping with the Growing Threat of Mega-Crises and Mega-Messes*. (Stanford, CA: Stanford Business Books, 2011): 101.