QFINANCE

Managing Operational Risks Using an All-Hazards Approach

by Mark Abkowitz

Executive Summary

- Operational risk management (ORM) enables an enterprise to understand, prioritize, and control risks that threaten its well-being and the livelihood of its partners.
- Although traditionally stove-piped within an organization, different operational risks share many common elements, providing an opportunity to consolidate ORM into a single all-hazards approach, one that is holistic and systematic.
- The key to effective ORM is to recognize and mitigate those risk factors that erode our margin of safety, so allowing situations to spiral out of control.
- A key first step is for an organization to perform an ORM physical, enabling the identification of reasonably foreseeable risks, benchmarking the current status of the ORM program, revealing gaps where the organization is vulnerable, and developing cost-effective strategies to address these gaps.
- Based on recent historical events and changing conditions in our world, bringing ORM to the forefront of an organization is more important now than ever before.

Operational Risk Management: A Definition and a Strategy

For the purpose of this discussion, Operational Risk Management (ORM) is considered to be the policies, methods, practices, and institutional culture that enable an enterprise to understand, prioritize, and control risks that threaten the well-being of the organization, its business partners, communities in which it operates, and society at large.

The cost of *poor* operational risk management can be excessive, considering that the occurrence of undesirable events can lead to fatalities and injuries; property loss; business interruption; clean-up, remediation and disposal; fines and penalties; future inspections; new regulations; long-term human health effects; environmental degradation; damaged investor, insurer, supplier, and customer relations; and loss of public confidence. By contrast, the cost of *good* operational risk management may be limited to investment in risk management benchmarking and needs assessment; resources allocated to control high-priority risks; and ongoing costs associated with ORM performance monitoring and evaluation.

The Need for an All-Hazards Approach

In many organizations, the approach to dealing with operational risks is stove-piped, with different entities having responsibility for different hazards. For example, environmental health and safety worries about toxicity exposure, legal is concerned with liability, human resources focuses on occupational health, executive management has its eye on business continuity, risk management addresses insurance, and research and development cares about design failure. As a result each group has its own priorities, separate resources are used to address each problem, and there is limited coordination. Yet, while each threat may seem quite different, when one takes a closer look at how these events evolve, there is remarkable similarity; that is, a pattern or “recipe” for disaster emerges. This situation begs for the adoption of a single “all-hazards” ORM approach, a process that is holistic and systematic in nature.

Risk Factors

Within a recipe for disaster, each ingredient can be thought of as an underlying risk factor that erodes our margin of safety. Once this margin of safety is exceeded, the situation is liable to spiral out of control. Therefore, management control of risk factors is at the crux of an effective ORM program. In attempting to manage these risk factors within an organization, it is helpful to group them into the following categories:

Design and construction flaws: If there is a flaw in the design process and it is not discovered in time, the system is prone to failure. Even when the design is valid, problems can still arise if the materials used to fabricate the system components are faulty or the components are not assembled properly.

Deferred maintenance: It is human nature to choose to deal with problems at a later time, especially if the system is not actually malfunctioning. Unfortunately, decisions to defer maintenance often lead to the failure of a key system component before the repair can be made, causing a serious accident to occur.

Economic pressures: Organizations typically manage a limited budget. When these resources are too scarce or spending is not controlled adequately, pressure intensifies to implement strict cost-cutting measures. This can lead to shoddy workmanship, the purchase of inferior quality materials, elimination of the use of backup operating and safety equipment, or management ignoring problems that arise.

Schedule constraints: When a deadline has been imposed, and the activity has fallen behind schedule, pressure to make up ground can cause the responsible party to turn a blind eye to important details. This situation often leads to the elimination of critical tasks, personnel trying to accomplish tasks in parallel that should be done in sequence, or not pursuing certain considerations in sufficient depth to fully understand their impact on safety.

Inadequate training: Because of a lack of adequate training, individuals who are prone to make mistakes may be placed in positions of responsibility. This in turn can either initiate or intensify a crisis situation. When there are personnel shortages, individuals may be thrown into an important decision-making role while covering for others, performing a function for which they were not properly trained. Because individuals tend to forget what they were originally taught and since processes change over time and require new learning, lack of retraining can also be a problem.

Not following procedures: When engaged in a repetitive activity, complacency can set in, and individuals tend to drift away from following formal protocols. Consequently, they either neglect to perform certain steps or invent other ways to accomplish the same task, often not considering the possible safety hazards caused by their actions. Failing to follow procedures can create a hazardous situation, one that is exacerbated by coworkers whose actions are based on assuming that those procedures are being followed.

Lack of planning and preparedness: Because of the luxury of time and the fact that a disastrous event may not have been experienced in recent memory, people tend to place a low priority on being adequately prepared for a crisis situation. All too often, little forethought is given to the variety of disaster scenarios that could reasonably occur and how to deal with them effectively. Even in circumstances where significant effort has been devoted to planning and preparedness, the product of this effort can be a written plan that is not practiced or updated, rendering it of little value when a calamity arises. Lack of planning and preparedness is one of the most common risk factors at play when something goes wrong.

Communication failure: Communication failures can occur at various stages, altering an outcome in different ways. When communication fails between members of the same organization, critical information is not shared, such as when one group decides to shut down a critical protection system for maintenance while another group is carrying out a dangerous experiment. Poor communication between organizations is also problematic. Finally, lack of communication with the public or the provision of inaccurate information can place people at risk either because they do not know the hazards they are facing, or because they are not properly advised on how to protect themselves. Along with lack of planning and preparedness, communication failure is the most common risk factor at play when something goes wrong.

Arrogance: Arrogance can rear its head in many forms, but usually appears as either the person in charge being driven to succeed for individual gain without sufficient regard for the safety of others, or an experienced individual who has become overconfident in his or her ability to deal with any problem that might present itself. In either form, arrogance can have serious repercussions.

Stifling political agendas: Government policies can have a powerful effect on the propensity for disasters. If these political agendas are hard-nosed, with little room for dialog and compromise, affected parties can feel that they have little recourse other than to resort to extreme and often hostile measures.

It is important to note that we, as humans, are involved in each and every one of these factors. While this implies that we contribute to the cause or impact of every disaster, it also means that we have an opportunity to control these factors more effectively to achieve a better future outcome.

Getting Started

A key first step is for your organization to have an *ORM physical*, essentially a comprehensive review of how operations are performed, what risks are present in performing these operations, and how these risks are presently being managed . This engages the organization in identifying “reasonably foreseeable” risks, benchmarking the current status of the existing ORM program, identifying program gaps where the organization carries the greatest liability, and suggesting strategies and tactics that can be implemented to close these gaps. Having a risk physical is important regardless of whether the organization’s ORM program is relatively new or fairly mature.

Case Studies

ORM Failures and Successes

There are several historic events that bring the failures and successes of operational risk management into focus. How could the event have been prevented? What could have been done to mitigate the impacts? What management controls have been implemented since the event occurred? Could it happen again? These are all legitimate ORM questions that, through hindsight, allow us to learn from experience and apply these lessons to deploying more effective ORM in the future.

Hurricane Katrina

During August 2005, Hurricane Katrina slammed into the United States, hitting the coastal areas of Florida, Louisiana, and Mississippi. A combination of storm surge, wave action, and high winds resulted in the destruction of buildings and roads in the affected areas. The impact of Katrina on New Orleans was unusually severe; portions of the city were left under 20 feet of water due to failure of the earthen levees and floodwalls that had been constructed to safeguard the city from this type of event. Hurricane Katrina caused nearly 2,000 fatalities and an estimated economic loss of $125 billion, in addition to displacing hundreds of thousands of people from their homes and workplaces. The destruction and loss of life in New Orleans, while initiated by the storm itself, cannot be attributed entirely to Katrina. Numerous failures of the city’s flood protection system due to poor design and construction, deferred maintenance, and a lack of funding left New Orleans susceptible to a hurricane of Katrina’s magnitude. As the city filled with water, the hurricane’s effects were compounded by insufficient emergency planning and preparedness, and the inability of responders to communicate.

Alaska Pipeline and Denali Earthquake

A major earthquake struck the Alaska mainland on November 3, 2002, along the Denali fault, which passes directly under the Trans-Alaska Pipeline. Had the pipeline ruptured, it would have resulted in spillage of up to a million barrels of crude oil a day in an environmentally sensitive area. Yet not a drop of oil was released. This potential catastrophe was averted due to successful ORM in both the design of the pipeline system and the quality of the maintenance, surveillance, and emergency preparedness. The pipeline design team, using extensive field data, devised a system such that it could survive a major earthquake should one occur during the pipeline’s projected 300-year operating period. As a result, a $3 million up-front investment in geological studies and corresponding design considerations helped to prevent an environmental disaster that could easily have topped $100 million in remediation costs. Concurrently, a comprehensive surveillance and maintenance system was implemented, capable of identifying problem locations in real time and dispatching crews accordingly. Moreover, emergency response was facilitated by a well-organized incident command system, contingency planning, and a training program.

Making It Happen

- Designate ORM as a core business practice within the organization by establishing the program at the vice-president level. The VP should be responsible for defining ORM policies and procedures, and for providing oversight of program activities.

- Organize an ORM committee, which reports to the VP, with membership that includes representatives from each element of the organization that has a designated ORM responsibility.
- Perform an ORM physical, and use it as a basis for defining program priorities, allocating resources, and implementing management control strategies.
- Monitor and evaluate ORM performance to determine whether program objectives are being met.
- Maintain ORM as a living process that is part of the culture of the organization.

Conclusion

We can ill afford not to recognize the new age of operational risk management, one based on a holistic and systematic approach to identifying reasonably foreseeable risks, establishing priorities, and adopting practical, achievable, and cost-effective control strategies. As history has taught us, we remain vulnerable to the occurrence of catastrophic events whose prevention or mitigation is within our control. Moreover, changing conditions in our world are posing new challenges that will require making tough risk-related choices. Adopting an all-hazards ORM approach does not mean that we will never suffer another tragedy. However, the prospect of that happening is less likely to occur once investments in prevention and mitigation have been made. The bottom line is that we can, and should, do much better at being a master rather than a victim of risk. All it takes is a more organized approach to takes is a more organized approach to managing the risks that affect our daily lives, coupled with a greater tolerance for unfortunate events that will sometimes occur no matter how hard we try to avoid or prevent them.

More Info

Books:

- Abkowitz, Mark D. *Operational Risk Management: A Case Study Approach to Effective Planning and Response*. Hoboken, NJ: Wiley, 2008.
- Garrick, B. John. *Quantifying and Controlling Catastrophic Risks.* San Diego, CA: Elsevier, 2008.

Websites:

- Risk World: www.riskworld.com
- Society for Risk Analysis: www.sra.org

See Also

Best Practice

- The Assurance versus Consulting Debate: How Far Should Internal Audit Go?
- Building Potential Catastrophe Management into a Strategic Risk Framework
- Countering Supply Chain Risk
- Everything You Need to Know About Benchmarking
- Risk Management: Beyond Compliance

Checklists

- Applying Stress-Testing to Operational Risk Exposure
- Creating a Risk Register
- Establishing a Framework for Assessing Risk
- Key Components of a Corporate Risk Register
- What Is Benchmarking?

Finance Library

- Mastering Risk, Volume 1: Concepts

To see this article on-line, please visit
http://www.qfinance.com/operations-management-best-practice/managing-operational-risks-using-an-all-hazards-approach?full