Funston Advisory Services LLC

3 Developing a Common Understanding

by Rick Funston and Randy Miller, May 21, 2014

Introduction

Kick-starting the dialogue about value and risk begins with five questions to be answered by the executive:

1. What are the major risks to our system?
2. Who is responsible for managing those risks?
3. How prepared are we to prevent or respond to those risks?
4. What can we do to practically reduce any unacceptable exposures given our limited resources?
5. How does the board know your answers are reliable?

We described how to answer the first two of these questions in the last article and provided a framework for risk identification and clarifying executive risk ownership. To address the remaining three questions, this article continues with a discussion of how to assess preparedness, identify and reduce vulnerabilities, build a business case for improved risk management and improve confidence in the reliability of these assessments.

3. How prepared are we to prevent or respond to a major risk?

"Focus on the icebergs, not the ice cubes"

Preparedness relates to the ability of the system to prevent, detect, respond and recover from a risk event. While there is no such thing as perfect prevention, the ability to prevent a risk from occurring is related to control over its causes. Is the risk caused primarily by external or internal factors? If the causes are largely external, you will have little control and may be unable to prevent a risk occurrence,

e.g., a hurricane. Instead, you may need to focus on mitigating the effects through advance preparation. In addition to any direct losses, reputations also suffer when an organization is not well prepared.

If the causes are primarily internal, e.g., people, processes or systems, you ought to have greater control over both cause and effect. In either case, how fast can you detect a risk occurrence? Are there early warning signs of its incipient stages? How good are your signal detection and pattern recognition capabilities? How fast are your response times? Does a response and recovery plan exist? Has it been recently tested?

If it is relevant, you should be prepared

Taking these factors into account, how prepared is your system to prevent, detect, respond and recover from a given risk if it occurs? If it is a major risk and it is relevant, then you should be prepared. Given limited resources, it makes sense that priority should usually be given to the risks that are already occurring or are most likely to occur. However, it is always a calculated risk as to whether a high impact but unlikely event will occur. Unfortunately, extreme risks are wildly random.

Speaking of investment risk, Noble Prize winner Eugene Fama stated *"If the population of price changes is strictly normal, on the average for any stock … an observation more than five standard deviations from the mean should be observed about once every 7,000 years. In fact, such observations seem to occur about once every three to four years."* [1] Or as Aristotle said "Expect the unexpected to happen often."

Just because you don't think it is likely, doesn't mean you shouldn't be prepared. History is littered with the casualties of those who thought disaster couldn't befall them.

Common policies about acceptable risk

Obviously, lower levels of preparedness for major risks increase exposure. Are there any exposures which are unacceptable? The determination of what is acceptable or unacceptable should be part of the executive dialogue with the board and reflected in the system's risk appetite and risk tolerance policy statements. This is discussed in the article on strategic risk and the role of the board.

As noted previously, the definition of risk often depends on the discipline. We define risk as the potential for failure that could result in loss, harm or missed opportunity. There is the risk of action but also of inaction. Forensic engineers define failure as an unacceptable difference between actual and expected performance.

[1] *Fama, Eugene The Behavior of Stock Market Prices, 1965*

If failure is an unacceptable difference between actual and expected performance, then what is acceptable vs. unacceptable performance? How much risk are you willing to take to achieve a valuable result? What is your appetite for risk? How much risk (failure) are you willing or capable of tolerating? For example, what is the risk of your fund failing to achieve its expected rate of return over a given time period? These are important policy decisions and while they can be difficult and prolonged discussions, they should be tied to the system's investment beliefs and capital market assumptions.

4. **What can we do to practically reduce any unacceptable exposures given our limited resources?**

Once there is an agreement on what is an acceptable vs unacceptable exposure, the next step is to determine what to do about unacceptable exposures. Leaving aside specific responses to investment risk, there are a number of ways to mitigate risk. Listed below are a few examples of prevention and detection controls:

1. Management review and approvals, authorizations, and verifications
2. Segregation of duties
3. Documentation and retention of records
4. Physical security of assets
5. Systems controls over information systems
6. Reconciliations
7. Reviews of performance
8. Direct supervision or monitoring of operations
9. Quality assurance
10. Independent reviews
11. Internal audit focused on the most significant risk and controls
12. ERM for program support and reassurance
13. Training and awareness
14. Policies and procedures
15. Risk transfer / alternative risk financing / insurance

Developing the Business Case

Sooner or later the issue of cost always arises and each of these controls has an associated cost. So how does one build the business case for improved risk management? For this reason, several years ago, I adapted a concept from Total Quality and renamed it the Total Cost Of Risk (TCOR).[2] There are two fundamental elements to the TCOR. The first is the Cost of Good Risk Management (GRM) which is the

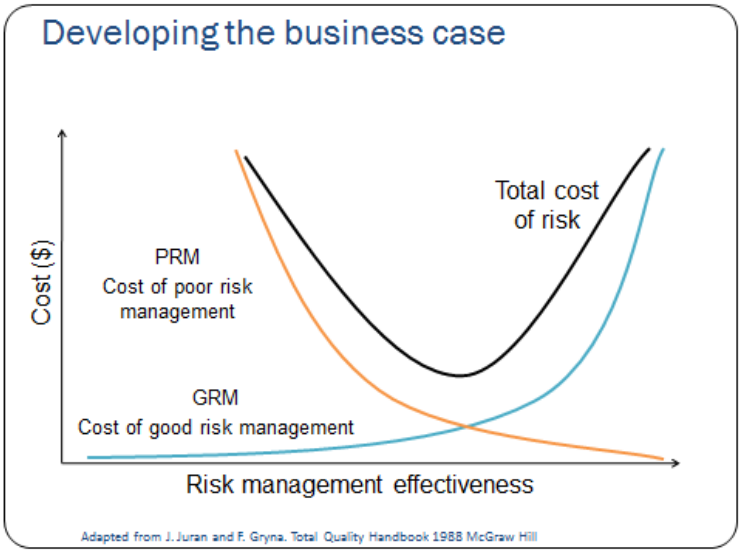
[2] "Surviving and Thriving in Uncertainty: Creating the Risk Intelligent Enterprise" Funston and Wager, Wiley & Sons. 2010.

cost of prevention and detection. The second is the Cost of Poor Risk Management (PRM) which is the cost of failure and response and recovery. Taken together, GRM plus PRM equal the Total Cost of Risk.

Every executive spends each day managing risk 24/7/365 whether they realize it or not. In addition to the time of executives spent on risk management, like the tip of an iceberg, GRM costs are the smaller but explicit, visible costs of Internal Audit, Risk Management, Compliance, Insurance, Business Continuity, Security, Legal etc. As such, they are always subject to pressures to save money. However, risk can never be eliminated and there is an efficient frontier at which no further value can be gained from increased spending on GRM and risk reduction as public companies have discovered with their spending on Sarbanes Oxley.

However, by far the larger cost is the cost of failure or Poor Risk Management (PRM). This is the too often unseen body of the iceberg itself. These are the costs of Response and Recovery from failures in asset allocation, portfolio management, operational processes and systems, procurement problems, conflicts of interest, due diligence, IT security etc. The costs of these failures often do not become visible until a crisis occurs and the damage must be controlled.

It is very hard to justify a business case in favor of increased investment in GRM if you don't know what the costs are of PRM. Just like quality, it is possible that if the costs of PRM are high, often orders of magnitude higher than the costs of GRM, then the reduction in the costs of PRM will more than pay for the investment in GRM. This is the argument for improving the effectiveness of risk management. See the chart below:



This chart shows that up to a certain point, the costs of PRM can be reduced by investments in GRM. However, after a certain points no benefits will result from further spending. Obviously, the risk mitigation methods chosen must match the nature of the risk. When faced with a number of risk

mitigation alternatives, one way to determine the most appropriate course of risk mitigation is to arrange the alternatives in a hierarchy from least to most in terms of factors such as degree of difficulty, expense and time required. A logical sequence of implementation is bound to emerge. Executives should then report back on actions taken and the results achieved.

5. How does the board know your answers are reliable?

Every executive risk owner should be expected to answer the preceding questions to the best of their ability and to provide reasonable but not absolute assurances as to their reliability. Naturally, there will initially be differences in understanding about, for example, the nature of the risk, the impacts it may have, the probability of its occurrence, the speed of onset, the costs of mitigation and the reliability of the assessment. However, common understanding will improve as a common language, common policies, common processes and common tools are developed and refined over time.

As mentioned in the first article, independent reassurance should also be obtained from parties independent of operating management that the executive's reports are reliable and that the controls are working as expected. Otherwise, fiduciaries may assume risks are being effectively addressed when the exposures actually remain high. This is how many boards are blindsided by risk they thought were under control. Independent reassurance typically comes from internal functions such as Internal Audit, Compliance, Risk Management as well as external third parties.

Common Language

Developing a common language of risk begins with common definitions. It starts with what you mean by risk. To improve consistency, many organizations develop a taxonomy or glossary of risks. A risk glossary typically describes the risk category, for example, financial, legal, operational, organizational, reputational or strategic.

Within the category of operational risk, procurement and contract management may be a sub-category, and "procurement risk" might be defined as "Procurement is not completed on a timely basis. Decentralized purchase order administration, inconsistent levels of purchase order payment authorization, or lack of centralized receiving/ monitoring/ reconciliation process result in receiving and payment risk."

The ERM program can help kick-start the development of a common language by providing example risk definitions. These should then be reviewed, revised and ratified by the respective executive risk owners both individually and collectively.

With its major risks identified and commonly defined, clear ownership and responsibility for risk management, an understanding of the current level of preparedness to prevent or respond to those

risks and a plan to reduce unacceptable exposures, the system will have an excellent basis for a continuing and important dialogue. The next article in this series describes how to make ERM enterprise-deep not just enterprise-wide.

About the authors. Rick Funston is the Managing Partner of Funston Advisory Services LLC which specializes in governance, strategy, and risk intelligence. Rick was formerly the National Practice Leader for Deloitte's Governance and Risk Oversight Services. He is the principal author of 'Surviving and Thriving in Uncertainty: Creating the Risk intelligent Enterprise" Wiley and Sons, 2010.

Randy Miller is a Principal of Funston Advisory Services LLC and former senior consulting partner with Deloitte for 27 years with extensive experience in strategy, benchmarking and operations improvement.

www.funstonadv.com