As featured in
The CEO Magazine
For more info visit
theceomagazine.com.au

Answers to the Top Ten Enterprise Risk Management Questions

BY GARY W PATTERSON

THE FAILED STRATEGIES OF WALL STREET FIRMS, JAPAN'S EARTHQUAKE, TSUNAMI, AND NUCLEAR PROBLEMS, ALONG WITH THE BP OIL SPILL, ALL DRAMATISE THE ACCELERATING PACE OF CHANGE AND UNCERTAINTY IN TODAY'S BUSINESS ENVIRONMENT.

In recent years, globalisation has increased foreign exchange risk. The failure of internal control mechanisms led to the compromise of Barings Bank and the destruction of Enron. In addition to the pervasiveness of globalisation and high-profile control failures, the advance of technology and the uncertainty of terrorism contribute to the escalation of complexity and risk in today's world.

In response, regulators, rating agencies, stock exchanges, institutional investors, and corporate governance have demanded that senior executives take more responsibility for managing risks for the enterprise as a whole. Increasingly, public shareholders are expecting stable and predictable financial performance.

With this environment, it behoves the enterprise to take a holistic view of risk management.

1. WHAT IS ENTERPRISE RISK MANAGEMENT (ERM) AND WHY IS IT IMPORTANT?

ERM is not an event or the responsibility of a few. Rather, it is a program that requires everyone in an organisation to do his or her part. Many businesses have an ERM program office that focuses on governance, control, assurance and risk management.

The scope of effort is broad and deep, while the overarching goal of ERM relates directly to the overall business objectives of the organisation. Its role is to see that the programs and controls are in place so that a reasonable person could expect that the firm's objectives would be met. It is designed to identify potential events that may affect the enterprise and manage risk according to the company's risk appetite. The process is applied in a strategic setting across the whole enterprise.

Informed by management's philosophy towards risk, risk appetite is then reflected in a company's overall strategy. For example, a start-up often has a greater risk appetite because it seeks high returns where success is uncertain, while a mature firm might seek smaller but more stable return for its investors.

Every entity exists to realise value for its shareholders; and this value is enhanced, maintained or reduced by management of all activities from the determination of strategy to the conduct of day-to-day operations. ERM enables management to effectively deal with potential events that foster uncertainty and respond in a way that reduces the probability of downside outcomes and increases the upside.

2. WHAT ARE THE INITIAL ELEMENTS OF AN ERM PROGRAM?

ERM establishes an overall risk management philosophy with the understanding that both unexpected and expected events occur, from catastrophic incidents to worker compensation claims.

The ERM function works with management to establish a conscious risk culture within the organisation, and appraises how the organisation's plans and actions affect the firm's risk profile. For example, a business may consider going into a new venture which is extremely risky compared to existing business. ERM can make sure that top management is aware of how the new business would affect the company's risk culture and the likelihood that its overall business objectives are met.

ERM also helps management take risk strategy into account when organisational objectives are set. They reflect the explicit risk appetite of the entity, and in the aggregate inform how much risk management the board is willing to live with so that risk tolerance is aligned with risk appetite.

At the outset, ERM leadership must come from the top with the development of philosophy, culture and strategy.

3. WHAT OTHER ELEMENTS OF AN ERM PROGRAM ARE NECESSARY?

Risk event identification is a key program element. These potential internal and external occurrences associated with the organisation could impact the company's strategy and achievement of its business objectives. The ERM function then looks at how these incidents could combine and interact to influence the company's overall risk portfolio. Through risk assessment, ERM looks at both the impact and probability of each event. Both quantitative and qualitative methods are used to assess risk.

In the context of both risks and objectives, ERM develops a risk response which identifies and evaluates risk options. The company's risk appetite, the cost benefit of response alternatives, and the extent to which a response diminishes the impact or likelihood of a particular risk, all inform the evaluation process.

Internal controls are key to any ERM program. This includes compliance with the separation of financial duties, quality control, and regulatory requirements. The company must capture and disseminate information in a form that allows individuals to carry out their jobs.

Finally, ongoing monitoring of program elements is integral to ERM, with follow-up by management oversight and periodic review. Risks must be identified and responses developed: internal controls, along with communication and monitoring, are necessary elements of an effective ERM program.

4. WHAT IS THE APPROPRIATE RISK CONTEXT FOR AN ORGANISATION?

Risk context is an entity's risk threshold, over which a particular action becomes 'risky' and under which it is deemed consistent with the firm's objectives.

For example, within an organisation the risk context for a new venture can be different for each manager depending on where they are sitting. For instance, the risk context for a geographical manager in an organisation may be one of slow but stable earnings growth, whereas the risk context for a product line manager in the same organisation may be one of high but fluctuating returns. So what should the risk context be for evaluating the new venture?

The answer is that neither the geographical manager nor the product line manager's risk appetite is compelling, in and of itself. The risk context for the new venture should be the context for the enterprise as a whole, whether it be from the view of the shareholder, employee, or customer.

5. HOW IS A RISK CULTURE DEVELOPED?

There is no 'one size fits all' for ERM. The organisation's management team must design ⋯›

ERM using a set of guiding principles. The efficacy of the risk management program is determined by the company's mindset where cooperation, talent and expertise are brought to bear on every aspect of risk.

Developing a risk management culture within the organisation is key. This requires training, supporting and communicating, and compensating risk-smart behaviour. If the risk culture is embraced by employees, they can help develop risk practices within their areas of expertise and have a unique vantage point to detect hidden risks in routine operations.

It is the board of directors that is responsible for making certain that senior management establishes risk management strategies. It is critical to the development of a risk culture that ERM be articulated at the level of senior management.

The chief risk officer who serves at the executive level must create a two-way dialogue throughout the organisation. With the implementation of an ERM infrastructure, line management is depended upon to perform the initial risk analysis. They can incorporate risk controls into business decisions to protect the company from inappropriate risk exposure.

The development of a risk management culture requires the investment of human and financial resources. It takes involvement by the board and senior management to ensure that ERM is implemented throughout the entire organisation.

6. HOW ARE POTENTIAL RISK EVENTS CATEGORISED?

The risk assessment must reflect the entity's objectives and its risk appetite. A portfolio view which considers risks in the aggregate for the organisation as a whole provides the context for placing particular risk events in a particular category.

Risk category has two dimensions: the potential impact and the likelihood of occurrence. For a specific organisation, examples of risk events for a given set of risk dimensions might be:

High impact–high probability: Credit risk or product obsolescence

Low impact–high probability: Data entry errors or equipment obsolescence

High impact–low probability: Loss of communications capability or an earthquake

Low impact–low probability: Lost records or power outage at noncritical facility

The categorisation of a particular risk depends on the nature of the firm's business. For example, credit risk for a seller of earthmoving equipment may be high impact–high probability, while credit risk for a direct seller of children's clothes may be low probability–low impact.

The impact and probability, along with the nature of a company's business, determines how a particular event is categorised.

7. WHAT ARE THE DIFFERENT TYPES OF RISK RESPONSES?

There is a range of options that an entity has for responding to a particular risk. Decisions about risk response within an organisation that has effective risk management are made in the context of a firm's risk appetite and a portfolio view of risks in the aggregate. The four types of risk response from which a company may choose are:

Avoidance: Stop engaging in the activity that creates the risk.

Reduction: Reduce the probability and/or the impact of a particular risk.

Sharing: Spread the risk among other entities.

Acceptance: Do nothing and subject the firm to the risk event.

Paying bribes to foreign officials is an example of a risk that might be avoided to preclude the chance of regulatory prosecution. Risk reduction would be the implementation of greater quality control to avoid a product recall. Classic examples of sharing the risk are insurance and hedging. And not implementing security practices in response to the threat of terrorism would be an example of acceptance.

Within ERM, each company has a menu of appropriate choices from which to plan responses to events in its risk portfolio.

8. WHAT ABOUT ERM AND IT?

A company with a strong ERM program protects its IT assets and secures other related service providers. The issue of trade secrets is involved when companies write their own code. Make sure that no-one can use proprietary code without permission. This means that developers sign agreements recognising the firm's ownership and agree not to share it.

The use of open source code which has evolved with the intention of it being available to everyone presents its own set of problems. If the company modifies the code and now deems it proprietary, make sure your legal department is apprised of the situation. There can be questions about the right to use a core piece of software. A company is also obligated to secure code licensed from vendors by granting access only to those who need it.

In addition to managing the risk associated with computer code, your confidential data needs to be protected and secured. Data on in-house systems needs to be encrypted and protected from hackers. Encryption makes the stolen data unreadable.

The type of data being loaded onto third-party systems needs to be understood from an ERM perspective. Examine your company's agreement with the IT vendor regarding what kinds of measures are being used to ensure confidentiality. Again, there are potential legal issues if confidentiality is violated. Often, the vendor insists on indemnification. Is this something that the company can live with? Make sure that legal is aware of the issues.

Both IT code and confidential data are assets that the company needs to protect and secure. The proper ERM role is to assure that the company and its vendors are doing their part.

9. HOW CAN DATA ANALYSIS HELP DETECT COLLUSION BETWEEN PURCHASING EMPLOYEES AND VENDORS?

Today's business environment has increased the likelihood of employee fraud. Individuals are under financial pressures like never before. Companies are trying to do more with less, so the financial segregation of duties may be compromised; and the unseemly bonuses on Wall Street can prompt a dishonest employee to adopt an attitude of 'It's okay to get mine'.

The major form of collusion that takes place between a procurement employee and a company supplier is the kickback where an employee receives cash or other forms of compensation in return for inappropriately influencing a company buying decision. This can include paying invoices for goods or services never received, bid rigging, or providing inside bid information to the supplier.

Collusion is hard to detect. However, data analysis can be used to spot unusual trends such as the number of invoices from a vendor over time, and the amount of dollars spent for goods and services from a particular vendor during a period of time when compared to previous intervals. This type of analysis can highlight scenarios that require further investigation.

10. WHAT IS THE BEST WAY TO WORK WITH THE MEDIA DURING A CRISIS?

Dealing with the media is a critical part of crisis management whether it is a fire, chemical spill or something else. In a high-profile crisis, the firm has a significant public relations risk.

It pays to be as transparent as possible. But this does not necessarily mean discussing issues such as liability or insurance. As part of a community, both the company and the media have a role to play, and it's in the company's short-term and long-term interest to help the news organisations do their job.

Excluding the media when a crisis hits is a big mistake because rumours and speculation will always fill a news vacuum. At best, the company looks like it has put its head in the sand, and, at worst, it appears guilty of something.

Often, it is advantageous for the company to take news organisations to the crisis site and tell the media what measures it is taking to deal with the situation. Remember, transparency often enables the firm to be portrayed in a favourable light.

It's critical that the company get out in front of the story by helping the media answer questions like who, what, where and when.

In conclusion, consideration of and the evaluation of your company's position relative to these Top Ten Enterprise Risk Management (ERM) Questions will enable you to understand your company's risks and how to respond to them, helping you to navigate uncertainty, while enhancing the likelihood of continued business success. ●

About Gary W Patterson, FiscalDoctor

Gary W Patterson, FiscalDoctor®, dramatically accelerates correct fiscal leadership decisions, working with over 200 companies during more than 30 years of top management experience in manufacturing, technology, wireless, service and distribution in companies including high potential, Inc. 500, middle market, and Fortune 500. Patterson has been interviewed or has presented internationally to groups and publications including Entrepreneur, Glass Hammer (UK), Directors & Boards, *Risk Management Magazine*, and *Top Producer*. He is the author of *Stick Out Your Balance Sheet and Cough: Best Practices for Long-Term Business Health* (tinyurl.com/stickoutbalance), and speaks on enterprise risk management, risk analysis, strategic budgeting, leadership, and change management.