Blakes
CANADIAN LAWYERS

ENTERPRISE RISK MANAGEMENT

By Mark Morrison

Shareholders, regulators, employees and other stakeholders expect management and boards of directors to avoid crisis situations, which are elevated in today's environment by the speed of technology, social media, increased shareholder activism, rapidly evolving regulatory requirements and opportunistic plaintiffs. Hackers, whistleblowers, activist investors and regulators also abound, and all seek opportunities that can be created by an incident that could have been prevented by a proactive approach.

More and more companies today are implementing "enterprise risk management" (ERM) programs, which utilize a proactive approach to assessment of organizational risks across all business lines and disciplines, a compliance plan to mitigate those risks, and crisis protocols to address issues when they do arise.

WHY IS ERM IMPORTANT?

Following the corporate scandals of the early 2000s such as Enron and Worldcom, it has become critical for companies to be proactive in their focus on corporate integrity and ethics—and ERM is a crucial element. Issues that can arise deep inside a company can quickly rise to become regulatory, reputational and/or even criminal in nature and can cripple a company.

A solid ERM program should proactively seek to mitigate against a variety of potential issues including:

- Regulatory issues. Environmental issues, antitrust, insider trading, anti-corruption sanctions and other compliance-related challenges all create risk.
- Resultant law suits. A regulatory issue can quickly become fodder for opportunistic plaintiffs' firms.
- Other legal issues. Plaintiffs are not the only risk. Corporate partners, suppliers and customers affected by the issues may also threaten litigation.
- Transactional considerations. Regulatory issues are often a key-gating item in transactional due diligence.
- Potential corporate issues, e.g., shareholder activism. Shareholders who believe the company has diminished value due to a regulatory or similar issue are in a great position to push a proxy fight, often resulting in a change in management or the splitting up of the company.
- Reputational damage. Nothing can cause a faster hit to the bottom line than reputational damage to the company. No company can succeed if it gives its customers too many reasons not to do business with it.
- Data and cyber issues. The risks of a data breach cannot be overstated. Employees, customers and others expect their information to be protected, and the financial costs of a failure can pale in comparison to the lost revenue and customer churn when they have lost that faith.
- Criminal matters. It is not uncommon for regulatory issues to rise to the level of criminal activity. A few missteps could land the CEO or other senior executives in jail.

THE ERM PROCESS

There are a number of steps to take in building an effective ERM program, but before embarking on any of them, it is critical to maximize the potential protection afforded by attorney-client privilege. While in many cases this may involve bringing in an outside firm as part of the team, the cost of doing so is miniscule compared to the potential of having the work product strewn across the front pages of the *Wall Street Journal*.

The six steps of a solid ERM process:

1) Risk Assessment

The starting point for risk management is to conduct a detailed and thorough risk assessment aimed at ensuring the organization understands the various risks endemic to the business and the various controls in place to address those risks. Identifying the gaps that may exist between risk and controls leads to the next step, which is developing strategies to eliminate those gaps or at least mitigate risk.

While there is no "one size fits all" form of risk assessment, they typically start with a desktop review and preliminary discussions with risk management personnel in order to identify buckets of potential risk, by country, region, business unit, industry, etc. Questionnaires or surveys are then often used to collect further information, followed by the most important step: interviews with those on the ground. Getting their input is critical, so part of the assessment process must include reaching out on a region-by-region basis and to as broad a group of employees as possible. It is the people on the ground who live with and deal with risks on a daily basis.

2) Planning

With the gaps between risk and controls assessed, the next step is to build a plan that includes strategies for closing those gaps by eliminating or mitigating those risks. It is important to build a customized compliance program with your overall business objectives in mind.

It is crucial to note that assessments may uncover risks that cannot be completely eliminated, even with the best possible compliance programs. It may also uncover behaviour that can be addressed going forward, but risks may remain from the past and a reasonable cost/benefit analysis under ERM may determine that the best path is to leave them alone. This is perhaps the single best argument for ensuring the entire ERM process is built under privilege. Should, for example, plaintiffs' lawyers ever find out that the company knew about a potential issue in advance but made the decision not to completely fix it, the damage could be incalculable.

3) Training

A crucial element of an ERM-supported compliance program is training: employees must be trained to avoid particular issues and risks, so training must be customized to the specific gaps that have been identified. Employees must understand the kinds of dilemmas that they may face and how they are expected to react when put in those situations.

In most circumstances, interactive in-person training is the best option. It provides an additional opportunity to spot issues and also ensures that the employees understand what the issue is, why it's important and why they need to care. Interactive in-person training, especially when built on a series of hypothetical circumstances rather than simple regurgitations of the law, allows companies to win the hearts and minds of their employees and arm them with the tools necessary to help keep the company out of danger.

4) Testing

Once an ERM program is in place, it is necessary to constantly monitor, review and improve its structures. Regulatory regimes change (or simply change their enforcement priorities), new products come onto the market, companies start doing business in new countries and the law changes, so frequent monitoring and testing of controls is integral to an effective ERM program.

5) Respond

Despite even the best efforts to eliminate and mitigate risk, emergent situations do arise. When serious criminal or reputational issues hit, there is a real risk of the company descending into chaos and making reactionary decisions that can aggravate the situation. It is crucial to have a plan in place ahead of time so there is a procedure to be followed during those stressful times. Simply having a plan is a calming influence, and it also sets up a procedure for making the right decisions and bringing in the right resources. Counsel, for example, can often bring the voice of calm rationality and a reasoned approach to a highly emotional situation along with the protection of privilege.

A good example is the fire drills we all went through in elementary school. While schools are built and plans are in place to prevent fires, there is still a procedure in place—practiced regularly—for when those plans fail. The result is that the kids know exactly what to do, how to behave and where to exit. A reasoned, practiced response plan can enable a reasonable response, even by kindergartners.

6) Improve

Once an ERM program is built and put in place, it is easy for attentions to be focused elsewhere. However, it is important to constantly look for ways to improve the program. This can often take place alongside the testing and monitoring phase. This may include auditing in new areas (both new business and geographies) and updated periodic risk assessments, all aimed at constant vigilance to make sure new risks are identified and gaps between those risks and company controls are filled.

ERM teams should also host closing meetings after each and every adverse event in order to improve the basic ERM structure, avoid similar problems in the future and make sure that the crisis response efforts were activated and worked properly.

CULTURE IS PARAMOUNT

Perhaps the most important aspect of a solid ERM program is not part of the process at all. It is the company's culture. A culture promoting ethics, compliance, risk mitigation and business integrity must be built from leadership on down. Such a culture enables an ERM program to work better and also helps to mitigate risk in places that may not be covered by a formal program. Employees that are trained and incentivized to "do the right thing" are more likely to do so, even if there is not a specific policy covering the situation.

The key phrase is "tone from the top," and it really is the key. Without the proper tone from the leadership and the board of directors, all of these structures put in place will be undermined as employees wonder if their bosses really desire compliance or if the entire program is an exercise in box-checking and rear-covering. Leadership must walk the walk by, for example, rewarding and not punishing those who bring problems to their attention. Only by constantly sending messages that they buy in can leadership win over the hearts and minds of employees. Fundamentally, the right culture is the foundation upon which all ERM is based.

THE FOLLOWING SITUATIONS are hypothetical but based in fact and representative of the types of issues that can arise without a strong ERM program to make sure there are no gaps between risks and controls.

1. The *New York Times* ran an exposé on an international company alleging a cross-border conspiracy. The activity was well outside the company's risk management program, so management learned about it from the reporter on the day before the piece was scheduled to run. The company was forced to devote enormous financial and reputational capital into the investigation, dealing with regulators in a variety of countries and fighting off the criminal prosecution and class action litigation that resulted.
2. A company in the process of doing due diligence for its initial public offering (IPO) uncovered an irregular payment scheme in a foreign country. It was forced to pause the IPO, investigate internally, and publicly disclose the scheme. The company's entire business plan was put on hold for several years while it was charged (and ultimately fined) and dealt with the resultant lawsuits and reputational damage.
3. A very large company had a whistleblower come forward who claimed that its international expansion was carried out through a wide-ranging bribery scheme. Rather than bringing the information to an outside firm to investigate, management decided to allow their internal team to do so, along with the company's general counsel in the country in question, who was alleged to be one of the parties involved. Growing impatient, the whistleblower went to the press, where the story focused more on the efforts to cover it up than the bribery itself. The company subsequently became the subject of an extensive regulatory investigation, shareholder class action litigation, and reputational damage resulting in a significant loss of market capitalization.

CONCLUSION

What's the return on investment from a world-class ERM program? It's hard to quantify exactly, but as of January 2015 one high-profile company had spent more than US$612 million just on the investigation of a single *Foreign Corrupt Practices Act* (FCPA) matter and the ensuing global review of its FCPA compliance program. This does not include any penalties, fines, settlements or judgments that may result, nor does it reflect any impact on stock price. In a number of recent cases faced by other public companies, the impact of a regulatory scandal on stock price was between nine and 11 percent—reflecting a potential for a loss of market capitalization in the hundreds of millions or even billions of dollars.

While such a scenario may be extreme, any company faced with a serious reputational issue also faces the potential for investigation costs, settlements, and potential loss of substantial enterprise value. The value of ERM may be hard to quantify, but the stakes could not be higher.

ABOUT THE AUTHOR

Mark A. Morrison is a Partner at Blake, Cassels & Graydon LLP (Blakes). He advises and defends clients with respect to white-collar crime, anti-corruption, competition and commercial litigation. He has substantial trial experience and has also directed numerous multi-jurisdictional internal investigations for public and private companies.

ABOUT BLAKES

As one of Canada's top business law firms, Blakes provides exceptional legal services to leading businesses in Canada and around the world.

For more information, please contact the author or any member of the Blakes Business Crimes, Investigations & Compliance group.