Bloomberg Law Reports® Risk & Compliance

Building an Enterprise Risk Management Program for A Small to Medium Size Company: Essential First Steps

Contributed by: Andrea Bonime-Blanc, Esq. Daylight Forensic & Advisory LLC

Introduction

We have all heard about ERM or Enterprise Risk Management especially in the past few years. ERM is the practice of building a company-wide risk management program to identify, manage, mitigate and eliminate a wide diversity of risks – from financial and operational risks to political and compliance risks. Whether they have formally put ERM into place or not, most large, international companies have some type of program in place developed organically over time. As these companies have encountered risks, they have developed mitigation strategies and tactics to manage such risks. Most of these larger, established businesses know that they need policies and protocols to keep up with the increasingly complex, unpredictable and risky business world.

Just because a company is relatively small or medium in size does not mean that it does not have a similar set of risks to confront in a business environment that is equally (or even more) complicated for smaller to medium size players ("SMC").[1] Indeed, in the absence of some form of ERM, the impact of an unidentified, unmanaged risk can be far more devastating to a SMC. A risk that blows up into an uncontrollable reputational or financial conundrum may be much harder for a SMC to tackle successfully and overcome because of the very size and resources available to a SMC. Thus an unattended risk can have an even greater impact on a SMC, threatening not only the viability of its current business cycle but also potentially its long term survival.

Larger, more established companies have had the relative luxury of time, resources, experience or regulatory pressure to develop strategies and programs to address risks. The same cannot be said for most SMCs. A SMC may not have been around for very long and has not become aware of the need for an ERM program. Or a SMC may not have the internal experience or resources necessary to create a formal ERM program. It is also possible that because a SMC does not have (or does not think it has) the same regulatory and legal pressures that a larger company has, building an ERM program does not appear on its radar screen. Or a SMC may have been lucky not to encounter a "life-threatening" risk yet and thus continues to do business as usual.

The bottom line is that SMC need an ERM program as much as larger more established companies do. We may be witnessing the beginnings of the next major micro-trend in global business as SMCs seem to be proliferating as a new, more nimble form of business in the 21st century. The advent and development of the Internet, social networking and other virtual tools has made it much easier to be a smaller player in a global business world. For these reasons and more, SMCs should attend to their risk profiles, understand how to address and mitigate their risks and build some form of customized ERM program into their strategy and corporate DNA. This article identifies six critical steps for SMCs to develop such a customized, useful and un-bureaucratic form of ERM.

Step I: Setting up a Risk Management Committee

The best way to set up a risk management committee is for two to three key leaders in a SMC – the chief financial officer, the general counsel, the controller, a business head, an operational manager or the chief operating officer — to get together to brainstorm who within the SMC would be best to include in a risk management committee ("RMC"). Depending on the expertise available within the company, the key business lines, the geographical spread and the extent of regulatory and legal risk, it should become clear fairly quickly who should form part of the RMC. The RMC should not have more than three to five members and should be a nimble body that avoids clutter, bureaucracy and inaction. The RMC can draw on additional internal (and external) subject matter experts from time to time who should be brought into meetings and projects for specific advice and analysis. It may also be useful to have a high level administrative person or junior business person become the "secretary" to the RMC to take notes, prepare reports and manage action items from meeting to meeting. Finally, the real work of the RMC will be done through a network of company contacts who will be the local or subject matter experts who will help to fill in the specifics of risk at the grass roots level of the company on an initial basis through an initial risk assessment ("IRA") as discussed below and on an annual or periodic basis thereafter.

Step II: The RMC Mission & Charter

Once the RMC team has been identified, the first order of business is to develop a draft mission statement and "charter" for the RMC and present this proposal to the chief executive officer and even the board or governing body of the SMC for approval and blessing. A simple yet effective mission statement might state something along the following lines:

> "The mission of the RMC is to identify, inventory and analyze the most important risks facing the SMC and develop an overall strategy and specific tactics to prevent and mitigate such risks on an ongoing and periodic basis."

The charter of the RMC can be a simple list of the following key elements:

A.) Who forms part of the RMC
B.) Who is chair and secretary of the RMC and how that role is assigned, rotated or otherwise filled
C.) How often the RMC meets and makes decisions
D.) The principal tasks and activities of the RMC
E.) Who the RMC answers to – the CEO, COO and/or board
F.) How often and to whom the RMC provides official ERM reports – whether interim, monthly, quarterly or annual

Step III: Embracing the Initial Risk Assessment

The next step the RMC must take is to identify a core group of qualified individuals in each business line or geographical area to be brought into the IRA process. They may be members of the operations team, controllers at each business or regional location, members of the legal team or other business functions. The key to success is to recruit responsible individuals who will work with the RMC on the IRA in a timely and responsible manner.

There are different ways in which the IRA can be conducted, but by way of an example, the following pieces should be included:

A.) IRA Project Manager. Appoint a project manager to conduct IRA. This can be a member of the RMC or someone else who is well organized and senior enough to command respect from the rest of the company.
B.) Q&A Document. Prepare IRA question and answer document providing the why's and what's of the IRA.
C.) ERM Framework. Have a document outlining the major categories of risk described in Step IV below, identifying some that the RMC has already singled out and asking questions to elicit further inputs from the business lines and administrative functions.
D.) Information Network. Create a network of competent information providers within the company. This group should be small but diverse enough to be able to tackle the wide variety of issues that may be identified as risks.

E.) Risk Brainstorming Sessions. Have brainstorming sessions at the business lines and/or geographical areas. These can be conducted ideally in person but also virtually through webcasts and other social networking tools.

Step IV: The ERM Framework: Identifying the Universe of Risks

Once the RMC has been put into place, the most important substantive exercise the team must tackle is identifying the SMC's universe of risks. Once the larger risk categories are identified, the more painstaking exercise of identifying specific risks can take place.

Each company has a different risk profile based on its business focus, geographical area of activity, whether it is publicly listed or not, highly regulated or not. and type of business. However, for most businesses the larger categories of risk will not differ substantially although there will always be a need to customize to the specific business. Table 1 provides an overview of one way to categorize overall business risks:

Table 1: **The ERM Framework: Identifying the Universe of Risk**
• Financial and Operational Risk
• Political Risk
• Governance Risk
• Compliance & Ethical Risk
• Third Party Risk
• Business Continuity & Crisis Management Risk

A.) Financial and Operational Risk. These kinds of risks lie at the core of the business. They would include the specific business cycle, contractual, inventory, supply and demand, credit, insurance and other financial and operational risks particular to the business. The inputs of leading business and financial people within a company including that of the chief financial officer, head of insurance, controller and specific business heads is critical for this exercise to be complete and properly focused.

B.) Political Risk. Depending on where a company does business, it will have to get its arms around what is called "political or regulatory" risk. Within this larger category of risk it is possible to identify several nuances:

i. The Government as Client. The risk of doing business with a government or one or more of its agencies (whether fully or quasi-governmental) with the attendant issues of corruption, bribery, procurement fraud.

ii. Political Stability. The risk of political regime stability in the regions or countries

it does business in.

iii. Violence. The risk of violence or other forms of bodily or property risk not only if doing business physically in that location but also if importing or exporting goods or services to that location.

iv. Regulatory and Judicial Transparency. The risk of regulatory and judicial transparency and predictability. In other words, is the institutional political framework within a country able to provide the SMC with a predictable and transparent set of rules or is a business at risk that if it has a contractual dispute with a local entity, for example, that it will receive independent and appropriate judicial treatment?

C.) Governance Risk. All companies have some form of governance – whether they are privately held, publicly traded, partnerships, limited liability companies, quasi-governmental entities, academic institutions or non-profits. All governance bodies need to act in a predictable and transparent manner through periodic meetings, the keeping of minutes, the passing of appropriately vetted resolutions and the proper vetting of conflicts of interest. The governance mishaps of many major corporations over the past decade have amply demonstrated that when governance is weak, a company can suffer seriously negative consequences.

D.) Compliance and Ethical Risk. There is a category of risk many businesses fail to identify in their ERM and which if left unidentified and unmanaged can create serious problems for a business up to and including dissolution. Table 2 outlines only some of the many ethical and compliance risk that should form part of any company's inventory of risk:

Table 2 **Examples of Regulatory, Compliance & Ethical Risks to include in an ERM**
• Antitrust and unfair competition
• Anti-bribery and corruption
• Anti-money Laundering & OFAC compliance
• Conflicts of interest vigilance
• Environment, health and safety
• Government and regulatory relations
• Harassment and discrimination
• Privacy compliance and data security
• Political lobbying. parameters

• Human rights and corporate responsibility
• Whistleblower mechanisms and protection

E.) Business Continuity & Crisis Management Risk. All companies have employees. All businesses – even the smallest, most virtual ones — have property, offices or other assets. Thus, all businesses need to have some form of contingency planning – for a physical location emergency (such as a natural disaster where employees live), a business emergency (when company records are destroyed by a computer crash), or a personal emergency (an employee has an accident while traveling on business). To avoid the risk of harm to employees and loss or destruction of company property, as well as to be able to restore business operations as quickly as possible in an emergency, all companies, including SMCs, must have some form of crisis management and business continuity plan in place.

F.) Third Party Risk. Third party risk is a category of risk that many companies don't think about until it is too late. There are several subcategories of third party risk that all companies should focus on:

i. Employees and Subcontractors. Employees and subcontractors must be vetted in advance to minimize or eliminate the risk of hiring people with criminal or other questionable backgrounds or having reputationally challenged individuals representing the business.

ii. Vendors and Suppliers. This is the risk of hiring suppliers or service providers who produce shoddy products (that can lead to product liability, e.g.), provide substandard services (that can lead to design failures, e.g.), or engage in illegal activities affecting the company (that can lead to accusations of bribery and corruption, e.g.).

iii. Clients and Customers. The primary risks involving clients include: (i) non-payment or late payment for products or services; (ii) insufficient, deficient or non-existent contractual rights when things go wrong; and (iii) client reputational damage that somehow becomes associated with the company.

iv. Business Partners. The risk with business partners is clear – if they do not conduct business with integrity, or they have credit issues, or there are significant lawsuits or liens against them, entering into business with them can not only taint a company but may also drag it into the partner's mess.

Most businesses will find these larger categories to be useful in building an ERM framework. However, depending on the business, there may be additional categories. A consumer products business would have a category for product liability risk. A pharmaceutical or health business would target the risk of not obtaining regulatory approval for new

medicines. For a business in the extractive or natural resources area, geological risk will be critical. And so on.

Step V: Translating Your Risk Universe into an Action Plan

Once the RMC and project manager for the IRA have gathered all possible information through the work described in the foregoing steps, it is time to pull it all together into a manageable, readable document that allows the risks to be clearly described and perhaps even measured or quantified. There are many and different ways to do this and it is not the purview of this article to review and describe all of these possibilities. Suffice it to say, that the key objectives of this part of the IRA exercise are to ensure:

i. That all relevant business lines, geographical areas and key functional parts of the business have had an opportunity to participate in the IRA
ii. That sufficient discussion has taken place at the executive level of the organization requiring input from the heads of the business lines and administrative functions
iii. That a carefully prepared and thought through IRA report has been put together outlining the major categories of risk and identifying and analyzing each major risk
iv. That all identified risks have been prioritized from most to least risky with a rationale as to why such a characteristic has been assigned to each risk
v. That for each risk identified there is a suggested solution or action item to mitigate or eliminate such a risk

Step VI: Embedding the Process and Answering to a 'Higher Authority"

The final and absolutely critical link in the chain of a successful ERM – no matter how big or small the company – is to tie the findings of the IRA back to senior management and the governing body of the company – its shareholders or owners, and board of managers or directors. Both at the beginning of the process – when a company decides to undertake an ERM, create a RMC and conduct an IRA – and at such time as the IRA has been completed to the satisfaction of the RMC, the governing body of the organization needs to be informed and their consent or blessing provided to secure the success of such an important undertaking. Communications with the governing entity should be formal and made part of the official agenda of their quarterly or annual meeting, especially when the IRA report is produced at the end of the initial risk management exercise for the SMC. However, an IRA is only the beginning of a successful ERM – after all it is the "initial risk assessment". Going forward, the RMC must continue to manage its risks proactively and periodically. It should undertake a new risk assessment – depending on the organization perhaps annually – that builds on the findings of the previous risk assessment and allows for the identification and management of new risks that have not been previously identified.

Table 3: **The Five Essential Steps to Create a SMC ERM**
• Set up a Risk Management Committee
• Create a RMC Mission & Charter
• Embrace the Initial Risk Assessment
• Identify the Universe of Risks and set up ERM Framework
• Translate Your Risk Universe into an Action Plan
• Embed the ERM Process and Report to Senior Management & Board

Thus, an SMC can have an ERM that is customized to its needs, isn't bigger or more complicated than it needs to be and isn't expensive to run as it makes use largely of internal resources. A successful ERM may also have a more subtle but nevertheless dramatic impact on the very existence and viability of an SMC: it can improve the bottom line by identifying risks before they blossom, it may avert the unraveling of an unattended risk that could threaten the very existence of the SMC and it can bolster the reputation of a business as a solid, ethical and reliable partner, supplier or service provider with a host of key stakeholders such as clients, regulators and employees.

Andrea Bonime-Blanc, Esq. is General Counsel, Chief Compliance Officer & Corporate Secretary of Daylight Forensic & Advisory LLC, an international regulatory and advisory firm. Ms. Bonime-Blanc is a member of the Board of the Ethics & Compliance Officer Association and recently co-authored/edited The Ethics & Compliance Handbook: A Practical Guide from Leading Organizations, published by the ECOA Foundation in 2008.

[1] In this article, SMCs are defined as companies with one or more of the following characteristics: (1) under 2000 employees; (2) under $100M in revenues; (3) privately or closely held; and (4) not highly regulated.