KPMG

The three lines of defense

Making the transition to a mature risk management model

Managing risk can be a dramatically different exercise for a company going public. While risk management is practiced in all types of sizes of business at some level, the greater the number of stakeholders involved, the greater the need for a mature and transparent risk management model.

Companies in the entrepreneurial and pre-IPO stages are typically "closely held corporations"[1] which are often well managed and controlled, but have a primary focus on business/financial risk. Since an IPO diversifies the investor community, risk thresholds need to be re-examined and aligned to meet the scrutiny of underwriters and the company's more diversified shareholders.

IPO companies should have a well-defined system that allows them to continue to make decisions that impact risk related to their changing strategies. A common and widely accepted method is the three lines of defense framework, which evolved after the 1990s (1995 to 2001) when the dot.com demise exposed the sheer breadth and depth of the risk landscape. This framework was designed to help organizations clearly identify the roles and responsibilities of the business units; practice ongoing risk management; and sustain risk management activities.

When applied properly, the three lines of defense create dialogue and analysis that prevents companies from overlooking risk factors that could ultimately cause financial disaster; as well as allow them to be proactive in how they manage risk within the organization.

The three lines of defense explained

The first line of defense consists of the business owners, whose role is to identify risk, as well as execute actions to manage and treat it. Pre-IPO companies by their nature are very oriented to this first line since typically owners will be very engaged in the daily business activities.

The second line is comprised of the standard setters or risk oversight groups (e.g., compliance functions, legal and enterprise risk management) which are responsible for establishing policies and procedures and serving as the management oversight over the first line (the doers).

The third line is comprised of independent assurance providers. These groups report independently to the board or the audit committee and include functions such as internal audit, external auditors, a Chief Risk Officer and special/ad-hoc committees.

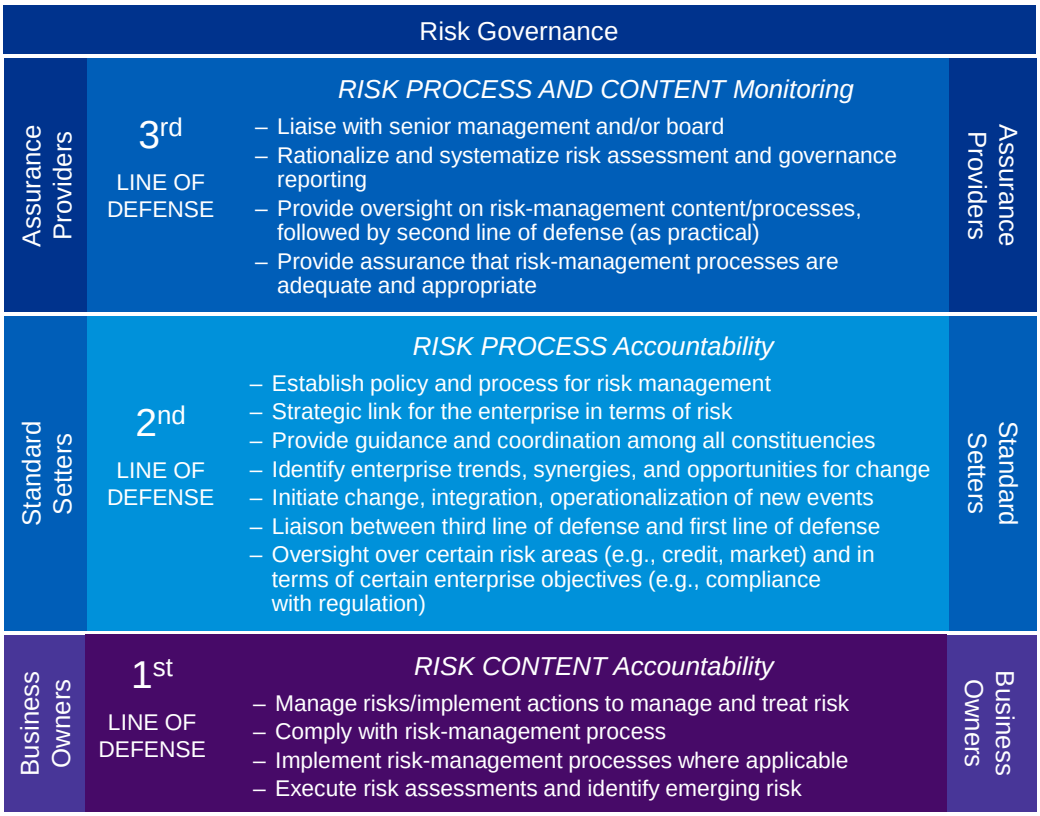
Making the transition

Small to medium-sized operations tend to view the three lines of defense framework as something more suited to large enterprises and financial institutions. However, as they move through the IPO cycle, they will be required to develop a more sophisticated framework to meet legislative and stakeholder requirements.

The transition to a mature framework does not have to happen overnight. Even a company in the pre-IPO stage has workable options that will allow it to transition to a three lines of defense model over time.

[1] See http://www.investopedia.com/terms/c/closely-held-corporation.asp for more information on the definition of a closely held corporation.

The three lines of defense framework



Knowing when the timing is right

The key decision is determining when the time is right to take your risk management model to the next level. That decision could be time or target-based based (e.g. when certain sales levels are reached or first expansion into a new market). Accountabilities can be shifted over time and be implemented in companies at varying levels of size and maturity.

I have often been asked by companies, why they need a three lines of defense model when they managed perfectly well before. The answer is a simple one: You always needed it. The good news is, with the right foundations, it's not as daunting a process as you might think.

Here's how it can be done:

1. Create a baseline. Conduct an initial risk assessment and formulate a simple dashboard outlining risks, controls, and the potential impact and size of each. This could entail workshops with management, as well as some external expertise and interviews (including with non-management individuals) to ensure as many issues as possible have been considered.
2. Process the information to understand and identify key vulnerabilities. Once those are understood, discuss them with management and assign some level of responsibility. Select five or 10 key risks/metrics that management will follow and define them clearly.
3. Ensure those metrics, monitoring activities and vulnerabilities appear in all reports and integrated during strategic discussions.
4. Review content on a regular basis and ensure that information is discussed, shared and incorporated into relevant content.
5. Engage other stakeholders – primarily the Board and Audit Committee. Here the discussion will focus on assigning responsibilities and more clearly articulating each line of defense and their responsibilities. Continue to discuss risk and the risk management framework on an ongoing basis.

Contact us

Doron Telem
National Leader, Risk Consulting
T: 416 777-3815
E: dorontelem@kpmg.ca