WHITEPAPER

The Puzzle of Risk Management: Fitting Together the C-Suite, Board and Internal Departments

The Puzzle

Risk assurance today is nothing like what it used to be.

Gone are the early days of risk assurance, where the external audit firm inspected financial statements and corporate compliance officers (assuming your firm had one) worked strictly on regulatory filings. The board simply reviewed the accuracy of audit and regulatory filings, and then talked strategy with the CEO.

While the Sarbanes-Oxley Act of 2002 birthed "compliance" as we know it today, the far more defining moment was the financial crisis of 2008 and all the regulatory change provoked by that transfiguring time. Today, virtually every participant in the corporate realm—regulators, investors, boards, employees, senior executives, internal auditors, external auditors, compliance officers, and others—are driving to a much broader goal of better risk management. The journey alone (never mind succeeding at that goal) will redefine risk assurance to its core.

We will begin with the beginning: how to work with your board to establish a basic structure of risk oversight, and what role compliance and internal audit functions play in that process.

The Most Important Principle of All

All a company's struggles with risk management can trace back to misapplying the concepts behind Principle 6 of the COSO 2013 Internal Control-Integrated Framework: "The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." (The framework has 17 principles in total, and the first five focus on the control environment. Principle 6 is the first of four principles on risk assessments.)

If an organization fails at this first principle of risk assessment—and we mean that literally; Principle 6 is the first principle in the COSO framework's section on risk assessment—then all your later efforts will fall short, because the parties involved will not have a clear, uniform sense of the goals they are trying to achieve or the risks they should monitor while trying to achieve them. You may have different parts of the organization disagreeing about priorities (compliance versus internal audit, for example; or compliance versus the business units). You may end up with a risk that exists in the company, but is tied to no specific objective, so nobody has the responsibility to manage it.

Setting clear objectives according to Principle 6 has become more challenging in recent years. Again, blame the financial crisis of 2008 and the change in regulatory thinking that followed. Prior to that, boards had been galvanized by the Sarbanes-Oxley Act to focus on compliance. The Dodd-Frank Act and all it hath wrought, however, are driving boards to focus on enterprise risk management—through much more elusive concepts such as "culture risk" (a favorite of financial regulators like FINRA today), or compensation schemes that encourage reckless decisions.

As a result, you no longer can treat ERM like a mapping exercise—which you could do with compliance. ERM is more a governance exercise, and we still struggle to articulate who oversees what: the CEO, the compliance and legal teams, the board, the internal audit department, the business lines.

We do know some broad contours of how to get started. First, the board as a whole should review business objectives proposed by the CEO (and his or her lieutenants, such as the CFO or COO). In theory, the next step would be for the audit committee to ensure that the risks to achieving those objectives are somehow managed. Or to put it another way, the audit committee sets the risk management and compliance objectives that should be achieved to help the company achieve its business objectives.

Two important considerations arise here. First, the audit committee itself doesn't have to oversee risk management; it only needs to ensure that some part of the board or company does. For example, NYSE's Listed Company Manual states: "The audit committee is not required to be the sole body responsible for risk assessment and management, but...the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken." Second, our description above ignores the reality that most businesses are not in a position to "get started." They are already in motion, and don't have the luxury of pausing to set clear objectives, assess risk, and then move forward. They must do the job within the company's daily operations.

All of that makes for a complicated dance to achieve the aims of Principle 6.

Applying Principle 6 to the Three Lines of Defense

In one way or another, most audit and compliance professionals have come around to the wisdom of the Three Lines of Defense model for risk assurance developed by the Institute of Internal Auditors in 2013: the first line are the business operating units; the second line are oversight functions such as compliance, legal, IT, and HR; the third line is internal (or external) audit. Some may quibble about where the CEO and the board fit into this picture; others wonder whether internal audit could handle some second-line duties of compliance. But the fundamental concepts—that the operating units "own the risk," while various management functions help the operating units manage risk, and some independent group also confirms risk management plans are working—are well-understood now.

That is risk management in practice. We simply need to tie the delivery of risk management back to the goal of Principle 6, which is deciding how you want to manage risk in the first place.

This is a project where compliance and internal audit are well-suited to divide and conquer: compliance can talk with the CEO about the importance of establishing a modern risk assurance program; internal audit can have the same conversation with the board or audit committee. Why? The compliance department often deals with urgent problems: investigations into misconduct; business processes violating some regulatory standard; the potential for civil litigation. The internal audit function, meanwhile, is more often seen as the audit committee's man on the scene, plus the internal audit team already is (or should be) conducting an annual enterprise risk assessment.

In truth, most CEOs and boards are quite receptive to talk about enterprise risk management and building a better risk assurance system. The trick is bringing them (and other relevant voices in the company) together to talk about risk assurance productively.

THE GROUP WILL WANT TO ACCOMPLISH THREE MAIN GOALS:

1. Declare what the business objectives are;
2. Declare what the risk and compliance objectives are;
3. Create a blueprint of who "takes point" on risk assurance day-to-day.

Consider the different priorities that different groups will have in this conversation. For example, the CEO might declare a business objective of "increase return on equity by 10 percentage points in the next three years." Boards, however, with their duties to investors who want no surprises in share price, might come to the table with an objective of "minimize unexpected earnings volatility." The goal should be to create a risk assurance function that achieves both objectives—or more precisely, a risk assurance function that lets the CEO achieve his business objectives within confines of the board's risk management objectives.

Some elements of that risk assurance function might be dictated to you. All registered investment advisers, for example, must have a compliance program, according to the SEC Office of Compliance Inspections & Examinations. All companies listed on the NYSE must have an internal audit function. Some of the duties those compliance officers and internal auditors should perform will be spelled out in relevant listing standards or agency regulations. Those are all facts of life for a large organization that must be accepted and even embraced.

The broader concern for a company, however, is this: How do you scope the duties of compliance and internal audit functions so they can usefully contribute to achieving those goals of Principle 6?

The keys to that answer are independence and authority: the more each function has, the better each function can find specific risks and assign them back to business objectives—which then forces the first line of defense (the business units) at least to consider those risks, even if solutions to managing them aren't clear. If compliance and internal audit can provoke those conversations, the organization's risk assurance function is moving in spirit of Principle 6. And Principle 6 itself moves in the direction that regulators today (and just about everyone else) want to go: toward comprehensive, enterprise-wide risk management.

After the Spirit Moves You

The details of scoping that independence and authority—whether to have a charter for each function; who reports to whom; how often each function briefs the board, and so forth—will vary enormously from one company to the next. In subsequent papers we will touch on some of those details, such as how compliance and internal audit can avoid duplicating effort, and how to take a risk management framework and build it into a "feedback loop" to help compliance and audit fulfil their missions.

For now, the parting lessons of this paper can be summed up as:

- Today's regulatory climate has shifted from a compliance-driven mindset ("Have we ticked all the boxes? Yes? Good, we're done.") to a risk management-driven mindset ("How can we ensure as best as possible that we avoid all unpleasant surprises?").
- Heed the concept behind COSO Principle 6: state business objectives clearly enough that the risks in achieving those objectives can be managed.
- Build a risk assurance function that is based on independence and authority for those in the second and third lines of defense who have daily responsibility for managing and monitoring those risks.