AGENDA
A Financial Times Service

Subsidiary Risk Needs Integrated Oversight

By Tony Chapelle
June 19, 2017

A significant number of companies — including Fortune 100 firms — continue to employ inconsistent methods of reporting the status of various risks that their subsidiaries and business units face, according to a variety of consultants in the field of governance, risk and compliance, or GRC.

Experts claim that a surprising percentage of companies are still working from spreadsheets, standards and taxonomies that differ depending upon the particular silo of the enterprise. These measurement methods, in turn, don't "talk" to each other well. Board directors therefore don't get an integrated viewpoint of the overall risks at all of the companies' subsidiaries or departments and how well they're being managed.

"I'd say that it's in the single-digit percentages of public companies that have a fully baked GRC program that supports effective risk management for the board to see," says French Caldwell, chief evangelist or marketer for GRC software at consulting firm MetricStream.

A former chief risk officer isn't much more optimistic. Nick Bednorz, founder and CEO of Comensure, a cloud-based platform for managing governance, risk and compliance (GRC) activities, says that only 10% of companies have integrated oversight of risk management for their operations. That's a key component of the "R" in GRC.

Without the proper systems in place, "boards can't get an integrated viewpoint of risk by definition," says Bednorz, who formerly served as chief risk, regulatory and compliance officer for Royal Dutch Shell's energy-trading business.

These and other experts advocate that boards insist on an integrated software program that can pull together reports and data from all the many departments and far-flung corners of a company. Those range from round-the-clock information gathered on regulatory compliance with laws such as Sarbanes-Oxley and Dodd-Frank to reports on IT risk management, business continuity management, internal audit for financial audits and operational audits for environment, health and safety.

"All these areas produce a lot of data about your risks and the controls you have to manage those. That data is being produced often to support very specific regulatory requirements," Caldwell explains. "Yet there are very few companies that have a complete and integrated GRC program. “But if you can put that data together and connect silos you give boards a more holistic view of risk,” he continues. “You can provide a look at the relevant assessments and controls and a much better view in real time of the overall enterprise risks that impact strategic issues that corporate directors are most concerned with.”

Benefits of an Integrated Approach

An integrated process can produce multiple benefits for boards and company leaders, says Deon Minnaar, the global lead partner for enterprise risk management and governance, risk and compliance at consulting firm KPMG. He says it “absolutely” reduces the footprint or duplication of effort of the enterprise’s management of day-to-day execution duties and controls. It also reduces duplication at the internal audit level; as a result, executives have a more integrated or overall view of the risks.

It also illuminates emerging risks more succinctly because you look across the entire business rather than in a silo. For example, if every division of the business manages cyber security purely in its own siloed way, the effect is that the enterprise has likely duplicated the effort multiple times. That has implications for actions such as allocation of capital to manage cyber risk. “By not being integrated, you might make decisions that won’t benefit the enterprise as a whole,” Minnaar concludes.

Spreadsheets that are created with the Microsoft application Excel are among the most prevalent non-integrated technology culprits at most companies. End user departments often create financial planning models in Excel for critical business activities that could easily impact financial and strategic risk. Yet employees can make changes to Excel spreadsheets without benefit of an audit trail. Such changes seldom go through any IT rigor such as security reviews, appropriate documentation or requirements for access rights, according to MetricStream. Therefore, risk management for business models has been coming to the attention of boards of directors, especially at major financial institutions.

In one remarkable instance, financial advisory analysts at Goldman Sachs in 2014 prepared a faulty spreadsheet that cost a client $100 million. Goldman was advisor for the cloud and software company Tibco as it put itself up for sale to Vista Equity Partners. The analysts created a spreadsheet that unintentionally overstated Tibco’s share count and thus understated its equity value per share. Vista Equity enjoyed a windfall at the expense of Tibco shareholders.

“We certainly feel that controls and governance needs to be at the board level,” says J.B. Kuppe, the head of marketing at software company BoardwalkTech. “A huge missing piece in most GRC deployments is control and access to the critical data that’s in spreadsheets.”

Kuppe says that most companies disclose in SEC filings if they have a GRC strategy and if there’s technology in place. Yet they don’t disclose its capabilities unless a failure arises, such as in a spreadsheet, and news about it ripples up in the press. Under Dodd-Frank regulations, financial spreadsheets for major banks must be discoverable, accurate and able to be audited. That requirement will likely ripple out to public companies in general.

“[At most companies] there’s nothing that lets you look into what’s happening in Excel, [yet] that’s where all the data decisions are being made for companies,” Kuppe emphasizes. “So, yes, this should be a board-level agenda for the [chief information officer]. Do you have effective control of your critical spreadsheets?” Her company is one of just a few, she says, that can provide that.

Once integrated GRC monitoring is implemented, Bednorz says, spreadsheets will be much easier to manage. “Now you’re able to consolidate all the information in one place for a real-time view of risks,” he says, “rather than wait for someone to change a cell in a spreadsheet or even different types of spreadsheets. Even the colors of the risk levels can change automatically.”

By contrast, Bednorz says, current enterprise resource planning (ERP) modules for governance, risk and compliance are so clunky, “I have never seen any of them work. That’s because they don’t get used.”

Pressing for Change

Some Fortune 100 companies still manage their risks in a silo fashion or use Excel spreadsheets because their functional departments, such as internal audit risk management or treasury, grew large and had mandates that didn’t necessarily include integration, explains Minnaar. “So now you have small empires that are built up across organizations.”

He says that in highly regulated industries, it’s been regulators that have pressed companies to upgrade to integrated GRC monitoring. On the other hand, in less regulated industries where KPMG advises companies, he’s seen that often the board is the catalyst.

That's likely because directors who have seen the benefits of an integrated approach because they sit on multiple company boards in other industries can help management ultimately understand GRC's benefits.

Finally, Minnaar finds that in what he terms "progressive" organizations, the management teams are pushing for an integrated approach to GRC.

Launching into integrated GRC isn't a walk in the park, however. Caldwell warns that the journey to a well-developed program usually takes three years. It typically takes that long for managers and the rank and file to embrace the organizational changes that come with implementation. That said, a company could start seeing benefits within six months.

Minnaar recommends that the CEO and C-suite clearly sponsor and own any launch. "Very powerful people have to work together and make change together," he emphasizes. "Start with an end in mind. You need a strategy to define success criteria. What do we decide success looks like?

"Ask who are your main stakeholders and how are they going to feel successful and not like they had to give up everything."

Lastly, Minnaar says, assign accountability at a relatively senior level that can't be delegated to lower-level managers. You need a steering committee that will drive integrated assurance of risk management.

"The mistake that people often make is not focusing on strategy first, but on technology. You have to start with strategy for integrated assurance. That's critical…. Technology enablement will follow."