23

Risky Business

LYN BOXALL

It may not be immediately obvious, but the governance role of boards has two dimensions: performance and conformance. Performance is about the company's strategy and value creation. Conformance is about risk management and regulatory compliance.

SUB-OPTIMAL GOVERNANCE

Too many boards spend a disproportionate amount of time on conformance. And yet, paradoxically, management and sometimes the boards themselves often feel their conformance actions are not as effective as they could be and that they are also a distraction when it comes to achieving the company's business goals.

For many companies, the result is ineffective conformance and sub-optimal governance. There are several reasons for this.

First, when management takes the position that conformance is a necessary evil and a cost that adds little value to the company's business, the conformance function tends to be under-appreciated and under-resourced.

The staff hired to ensure compliance may not be properly skilled or qualified. They tend to end up "ticking the boxes" rather than ensuring substantive and effective conformance.

Secondly, many risk managers and compliance officers see their roles as watchdogs, raising issues that are show-stoppers. They focus on defining "what cannot be done" by way of risk taking, and "what must be done" by way of internal controls. They then check that what cannot be done is, indeed, not done, and what must be done is done.

What should instead happen is for the risk and compliance functions to look constructively at business processes and, when confronted by "it cannot or should not be done", suggest more effective alternatives that are aligned with business objectives and risk appetites.

Thirdly, over time, larger organisations build up a plethora of conformance functions and staff that go by different departments and titles: internal audit, risk management, regulatory compliance, legal, etc.

These fragmented functions are usually managed independently and within silos. Each does not necessarily know what the other is doing. They duplicate work while leaving gaps. For example, a corporate function may be audited and assessed by multiple groups on an annual basis with significant costs being incurred and disconnected results.

ENTER GRC

With the conformance function facing increasing demands from regulators and calls for greater accountability, a concept that seeks to enhance and integrate governance, risk management, and compliance (GRC) functions within the company has caught on.

Increasingly a popular notion with companies in the US and Europe, GRC is essentially a system of people, processes and technology that enables an organisation to improve its governance through more effective compliance, and a better understanding of risk in business performance.

While the concept is relatively new and evolving, several elements of a good GRC framework bear mentioning.

To start, there should be an active governance structure that drives accountability in day-to-day operations so that the board and management have a proper degree of insight into key risks. With the appropriate level of information and understanding of the risks and options, boards and management are in a better position to make informed business decisions.

Supporting this governance model should be a sound system of risk profiling and reporting. The types of risks, mitigating options, and controls need to be defined, monitored and reported to management and the board.

It is crucial to obtain a clear understanding of risks across the company. This allows for an integrated approach that reduces gaps in risks and compliance processes, reduces redundancies, and gathers and presents GRC information quickly and consistently.

Risks need to be balanced with business opportunities and growth. While excessive risk taking should be avoided, some level of risk taking in line with the company's risk appetite is needed. Similarly,

the cost of controls needs to be balanced with the errors they are designed to prevent.

Good people are needed to drive an effective GRC. Towards this end, standards, training, and certification by industry bodies and third parties are increasingly available to those involved in GRC work. A leading example is the GRC Capability Model for Principled Performance, and related GRC Professional and GRC Audit certification programmes of the Open Compliance & Ethics Group.

HOLISTIC APPROACH

A number of third-party GRC software solutions are available in the market. These range from point solutions for a single function to integrated solutions that maintain a central database of compliance controls but manage, monitor, and present them against every governance factor. Technology and tools like these often make much of the compliance work more efficient. They play a vital part in supporting GRC, though care must be taken that they do not become the tail that wags the dog.

In summary, the three pillars of GRC – governance, risk management, and compliance – work together to help ensure that a company meets its business objectives. As a governance tool, GRC adopts a holistic top-down approach that supports the company's goals, as opposed to a bottom-up approach that works in isolation.

It is also an approach that optimises risk management and compliance efforts so that they are more cost-efficient. And that may well be the best reason to support its development and implementation. ■