JANUARY 2017

RISK

Nonfinancial risk today: Getting risk and the business aligned

Both must be deeply involved to avoid costly errors.

Joseba Eceiza, Piotr Kaminski, and Thomas Poppensieker

Ask senior managers at any company if they have nonfinancial risk under control, and the answer is likely to be yes. But as managers of companies in automotive, banking, oil and gas, pharmaceuticals and many other sectors can attest, the reality is often very different. And as personal liability for corporate actions takes hold, board members—both executive and nonexecutive—are on the hook not just for their personal involvement in risk- and compliance-related issues but also more broadly for the company's whole risk profile and enterprise-wide compliance.

Nonfinancial risk[1] has typically been addressed by one-off showcase initiatives based on a specific regulation or requirement, and left to experts in each field. What principles exist typically focus on adhering to formal standards and providing evidence that appropriate controls are in place. They are usually not embedded into the business but are instead delegated to risk and compliance departments, which have a limited understanding of how to manage risk and compliance within the business context.

In other cases, the business takes all the responsibility for managing risk, but without any link to the company's formal compliance, risk, and control framework. Quality control, for example, is embedded in the day-to-day management of manufacturing organizations, but those responsible are not involved in determining enterprise risk, leaving a major gap.

Both shortfalls have led companies from all sectors to be caught off guard when failures occur. And

those failures have led to catastrophic incidents and destroyed shareholder value time and again. Over the past 15 years, companies around the world have ended up in dire predicaments through such control failures. In all these cases, the formal risk-management approach has been criticized for being insufficient. In concrete terms, litigation and settlement of nonfinancial risk-control failures have cost the financial-services and corporate sectors several hundred billion dollars over the past ten years—and that does not include the additional impact of reputational damage.

The impact on management has been just as significant, including damaged reputations and personal prosecution, not only where senior management has been directly linked to wrongdoing but also where it was found not to have established a robust approach to risk and control management.[2] As this article will explain, there is a better way—one that needs to be adopted before a major incident occurs, and not after.

Risk matters, but not in isolation

Leading companies have established frameworks for risk and control management (R&CM) that help management balance the risk-management imperatives and the needs of the business—in other words, an approach to risk that accurately reflects the business context, while ensuring that risk and compliance management is embedded across the entire organization. This means going beyond implementing yet another checklist or improving the links between business units. It requires an explicit management dialogue about nonfinancial risk—about where it can occur and how it is being mitigated—and extends to questioning where the cost of control may be too high, given the value at stake. For many companies, this implies a full cultural transformation, so that a new set of risk-management processes can be as effective as possible. Until that changes, the same mistakes will be repeated year after year, and companies will be at risk as the threat to their value is overlooked.

Key objectives of a well-founded framework

Risk managers may argue that the basic principles of R&CM are well established, and indeed enshrined, in industry standards. The concepts may indeed be broadly known, but they are applied in such a scattered fashion that they are not fit for purpose. A board that wants to get on top of nonfinancial risk management needs to have three clear objectives:

- It must facilitate better decision making. A robust R&CM framework should help management better understand the company's risk profile so that it can make informed decisions, such as where to accept risk and where to mitigate it in the context of overall risk appetite and risk strategy. The framework needs to help businesses prioritize the risks and controls to address, based on their likelihood and potential impact on the business. It should form the basis for continuous risk management through a business view on value chains, processes, and embedded risks and controls.

- It must provide evidence for internal and external stakeholders of the adequacy of the controls that are in place (or that should be implemented), and it should clarify who is responsible for what regarding risk ownership and control execution. This gives senior management a way to assess the effectiveness of the organization, delegate responsibilities, and address legal implications.

- It must reinforce an adequate risk and compliance culture that should be as deeply embedded into a company's management approach as revenue and cost management.

The resourcing and costs of the R&CM approach should be aligned with the company's structure, business model, and risk profile. For example, an oil and gas company might choose to focus on regulatory and counterparty risks in markets where it operates, while financial firms might target product mis-selling. The approach should also provide guidance on the efficiency of the control environment as much as its effectiveness, by showing, for instance, the gap between the inherent risk and the residual risk after the control is implemented.

The business case for R&CM

Assessing, managing, and mitigating risk must be justifiable on business grounds. Running an effective and efficient R&CM, in our experience, can deliver a payoff of more than ten times the investment. There is no doubt that implementing R&CM is beneficial for companies across all industries. It can help reduce losses and the cost of control, which together should more than offset the up-front investment needed to set up the methodology and the recurring costs of maintaining it. And regulators approve, too.

Cut your losses

Organizations typically experience five types of losses from nonfinancial risk: recurring low-severity losses (such as credit-card fraud); one-off, high-severity losses (for instance, senior-management wrongdoing); regulatory fines; the imposition of greater capital requirements for banks; and reputational damage (where examples are legion).

A sound R&CM framework helps to reduce these losses by ensuring the right controls are in place. For example, a company might develop a coordinated plan with its telecom providers to prevent and counter distributed denial-of-service attacks, or take out insurance against cyberattacks. Preventing or reducing the impact of risk also reduces remediation costs—such as the cost of reviewing thousands of files or of setting up call centers to handle customer complaints. R&CM also helps reduce regulatory fines and can help smooth the conversation with supervisors.

Spend less on mitigation

At the heart of a strong R&CM framework is the prioritizing of risks and controls. This means that resources are focused where they will have the greatest impact and that duplicative controls are removed. In automotive, for instance, quality control is vital in production processes, but not all processes are equally important; therefore, it is important to invest in controls where both the likelihood of a risk event and the resulting impact are highest.

Aside from cherry-picking the most critical controls, an R&CM framework that has a unified and aggregated risk-assessment system immediately makes the control function more efficient and cost effective. This is essential when 5 percent of the workforce can be employed in control-related activities.

Identifying key risks also helps ensure the right insurance policies are in place. In addition, those policies should be more efficient and cheaper, because risk identification is more targeted and because it becomes clear how specific controls help mitigate risk.

Keep setup costs low

Setting up an R&CM framework is typically a multiyear effort, but strong management focus will ensure maximum effectiveness and efficiency. Furthermore, consolidating different control frameworks can deliver significant synergies from aligned management processes, system consolidation, and integrated reporting. Most important, setting up a robust R&CM framework permits a sharper focus on identifying and mitigating risk, through an objective fact base and

clearer policy standards. If set up properly, it also provides all the evidence required for the formal reporting to the risk or audit committees under COSO, ICS, ERM, or CMS standards.[3]

The regulatory benefits

A strong R&CM approach not only makes good business sense—it's also becoming more of a legal requirement. Several international regulators are pushing for clearer definitions of, and better connections among, the "first line of defense" (the business), the second line (the risk and compliance functions), and the third line (internal audit). This three-lines-of-defense model is increasingly used as a way of explaining the relationship among these functions and as a guide to how responsibilities should be divided.

How to get it right

The key components of a best-practice R&CM approach revolve around unified taxonomies, assessment tools, data and reporting tools—and ultimately the process that ensures the framework becomes part of the whole company's day-to-day life.

Get everyone talking the same language

Very few companies have a truly unified way of talking about risk or controls. Comparable risks may never be recognized as such, simply because they are described differently by different parts of the business. This can be as simple as, for example, identifying employee behavior and employee conduct as identical, when, in fact, the two are never linked—and thus the total risk level is misreported. Clear risk definitions need to be shared across the company in order to identify which risks to actively manage and monitor.

Exactly the same problem applies to controls. For example, identity control and access-management control might mean the same thing in the same company, but if that is not recognized, then their relevance could be underestimated.

The challenge is to ensure that the taxonomy is at the right level of granularity to help identify risk, but not so granular that it becomes unwieldy.

Map the risk

Once everyone is using the same language, the company can then identify where material risk for the organization exists.

A groupwide process map that represents the company's business model is a good starting point. Companies often struggle to find the right level of granularity in process maps: too high a level (for example, eight or nine processes for the entire institution), and the maps are of limited value; too granular (for instance, more than 100,000 processes at one European bank), and the effort required to create and maintain them is too burdensome. Mapping at the value-chain level is typically a good way to begin, and then, over time, the exercise can become more granular.

At an automotive manufacturer, for example, the first step was to identify and define specific compliance requirements by country (such as emissions, certification, and safety) and to understand their importance for car models across their life cycle. These were then mapped into the company's processes (from R&D to manufacturing), taking into account the complex structure of the supply chain, which involved dozens of nodes and locations.

Using the map and the risk taxonomy, therefore, a business can profile the risk in each process and assess both the probability and severity. This information is aggregated from the R&CM unit level to the enterprise level.

Understand the controls

Knowing which risks exist is only half the equation. The other half is knowing how to mitigate them. Organizations struggle to tie controls to risks for many reasons, which range from unclear definitions of controls to a limited understanding of how effective the controls actually are. This means that the business reviews hundreds of controls. But without a clear view on which are the most relevant and effective, no clear management perspective on the overall control strategy will be developed. To take an extreme example, in a nuclear-power plant, controls that monitor the performance of the core should have a much higher priority than controls that focus on avoiding outages on steam turbines through preventative maintenance. Both matter, but not to the same extent.

If an organization assembles only a list of controls, with no hierarchy, then that list is useless for management decision making within the business—and instead only serves as a way for compliance or risk functions to document the weaknesses that it identifies.

Leading players, therefore, undertake a fact-based control assessment: they find out which controls are used to mitigate which specific risks, determine how effective and efficient they are, and link them to the policies and operating procedures that clarify control standards, accountabilities, and training and communication that ensures the organization is fully aware of the risks. The assessment should draw on multiple sources of data, such as internal and external loss and incident data, audit-review results, supervisory findings, key risk indicators, and key control indicators.

Report back—and act

To make sense of the assessments, management must have a consistent view of nonfinancial risks and the underlying controls, with systematic reporting to the board. This requires an integrated management information system. Typically, these are bespoke versions of externally available packages that broadly match the company's specific R&CM requirements, or internally developed platforms. When selecting commercial packages, companies must be careful not to tailor them to a point where system upgrades become difficult to manage.

Where identified risks fall outside the company's risk appetite, concise and action-oriented risk and control reporting recommends where, how, and when the risk is mitigated. The actions might range from redesigning the entire control environment to reinforcing supervisory responsibilities, or even removing the product or process that is creating the risk. Ultimately, the reporting, based on the risk and control assessments, should enable the company to prioritize controls, based on specific context. Of course, any change to a control must happen within the organization's existing control framework in order to retain clear accountability.

Run the process company-wide ... and keep running it

As we saw at the start, the R&CM framework must be applied across the entire company, otherwise individual units, functions, or people can inadvertently create enormous risk. The process also needs to be aligned with both the company's management and accountability structure and its fundamental business processes and value chains. This way it can identify individual risk by area as well as control dependencies across the value chains (which extends to outsourcing arrangements via third parties).

Business units are prone to receiving overlapping requests to assess the risk of particular processes and assets from different risk-management groups (for example, cyber risk, or operational

risk). By coordinating and sharing information, the operational impact of participating in the R&CM processes is reduced, which leads to higher-quality risk information. Nevertheless, organizations can end up running hundreds of workshops each year as they attempt to identify risk and controls, and therefore clearly defined process and expectations for business units and control functions are crucial. Careful planning of R&CM entities and identifying those with similar profiles (such as all sales or production units) becomes paramount.

An annual risk-assessment exercise will never be sufficient; what's needed are both "trigger-based assessments" when incidents occur, when certain indicators breach thresholds or processes change, and ongoing monitoring. The model needs to be particularly strong given the interaction between the business-division risk owners who identify and assess the risks (the first line of defense) and the control functions who challenge the results (the second line of defense).

As senior management's personal liability for corporate risk increases, the traditional way of tackling nonfinancial risk management could leave many facing uncomfortable times in front of their boards, their regulators, and quite possibly their courts. A new framework for risk and control management is needed—one that is cost effective and explicitly ties risk to business value, and one that helps management have a fruitful conversation with stakeholders.

The risk and control management approach outlined here achieves this. By bringing the business into the risk-management discussion, corporate risk changes from a topic that someone else worries about to being a keystone of every employee's role in the organization. ■

[1] For the purposes of this article, nonfinancial risk is broadly defined as all risk that is not balance-sheet related (for example, excluding credit, foreign-exchange, commodity-price, and liquidity risk). Nonfinancial risk comprises compliance risk (for instance, the requirement to adhere to all relevant rules and regulations, and operational risk, such as process, production, technology, and cyber risk).

[2] This is reflected by the "business judgment" rule, which requires company management to establish processes regarding risk and compliance that are in line with industry practices for a business model of their complexity.

[3] COSO: Committee of Sponsoring Organizations of the Treadway Commission; ICS: frameworks for the internal control system; ERM: enterprise risk management; CMS: compliance management system.

Joseba Eceiza is a partner in McKinsey's Madrid office, **Piotr Kaminski** is a senior partner in the New York office, and **Thomas Poppensieker** is a senior partner in the Munich office.