Corporate governance and risk management: the growing importance of 'business integrity programmes'

Estibaliz Aranburu Uribarri

Partner, Corporate and Commercial and M&A Practice Areas, Gómez-Acebo & Pombo

As a consequence of the lessons learned from the recent crisis, one of the matters that draws most attention in the field of corporate governance is the responsibility of boards of directors over risk control and management policies. Comprehensive legal (statutory and regulatory) compliance and business ethics programmes, i.e. business integrity programmes, are essential in this context inasmuch as respect for the law and ethics in business are considered to be inextricably interwoven with adequate risk management.

1. Introduction

Although there is no 'one-size-fits-all' model, it is generally accepted that corporate governance should be conducive to: (a) generating maximum profitability for the company's shareholders; (b) ensuring said profitability and the company's mid- and long-term sustainability; and (c) rendering the achievement of the above objectives compatible with the company's fulfilment of legal, contractual and social obligations. The recent crisis, however, revealed that many companies did not have adequate corporate governance since, in some cases: (a) members of boards of directors were not professionally qualified to take on management or supervision of management, or did not sufficiently inform themselves of the companies' affairs or did not devote sufficient time to their office; (b) the systems of remuneration for directors or executives stimulated the obtainment of short-term profits, encouraging actions that could jeopardize companies' financial stability or long-term sustainability, whilst mechanisms to prevent rewards for poor performance were absent; (c) transparency was lacking with regard to directors' remuneration, conflicts of interest and related transactions; or (d) unethical behaviour, reckless actions or the taking of excessive risks were permitted or, at least, uncontrolled.

Faced with this reality, international organizations and national legislatures have reacted by driving forward legislative changes and best practice recommendations on the subject of

corporate governance. In this regard, one of the matters most addressed, particularly by the OECD, is the role of boards in determining corporate strategy and risk management (in other words, the responsibility of boards over the management of corporate risks) and, tied to this, the importance of legal (statutory and regulatory) compliance and the need to foster ethical corporate behaviour, inasmuch as respect for the law and ethics in business are considered to be inextricably linked to adequate risk management and long-term sustainability of companies.

Below we will refer to a company's set of programmes, protocols, functions, persons, procedures or internal controls, with regard to ethical culture, legal compliance and risk control and management, as business integrity systems.

2. Legislative bases of business integrity programmes

In our setting, the Companies Act Amendment (Corporate Governance) Act 31/2014 of 3 December[1] ("Act 3172014") introduced art. 529 *ter* (1), whose sub-articles (a) and (b) state, inter alia, that the following are non-delegable powers vested on boards of directors: "the corporate social responsibility policy" (which, according to recommendation 54 of the Code of Governance of Listed Companies[2], should include mechanisms for supervision of non-financial risk, ethics and business conduct) and "[t]he determination of the *risk control and management policy*, including of a tax nature, and the supervision of internal information and control systems". On the other hand, the Code of Governance of Listed Companies highlights the concern shown on this matter by both the OECD and the EU and its capital importance, hence its inclusion of principles and recommendations regarding risk control and management and the supervision of corporate legal compliance and ethical behaviour.

As regards unlisted companies, art. 249 *bis*, introduced by Act 31/2014, adds to boards' non-delegable powers "the determination of the companies' general policies and strategies"; contrary to what happens in the case of listed companies, specific policies are not included. In our opinion, this does not mean, however, that in unlisted companies business ethics, legal compliance and risk control and management policies are not non-delegable powers of their board of directors, to the extent that these are general policies or strategies of companies. We arrive at the same conclusion if we consider the following:

(a) The explanatory notes to Act 31/2014 refer to the increasing importance of risk management, which is directly related to a well-managed board.

(b) Art. 217(4) of Royal Legislative Decree 1/2010, of 2 July, approving the Recast Text of the Capital Companies Act[3] ("LSC"), provides that "[t] he system of remuneration established [for directors] must be aimed at fostering the company's long-term profitability and sustainability and must incorporate the necessary precautions to avoid excessive risk taking

[1] *Ley 31/2014, por la que se modificaba la Ley de Sociedades de Capital para la mejora del gobierno corporativo.*

[2] *Código de Buen Gobierno de las Sociedades Cotizadas.*

[3] *Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el Texto Refundido de la Ley de Sociedades de Capital.*

and the rewarding of poor performance", based on which it is also clear that directors are responsible for: (a) fostering the company's long-term profitability and sustainability; and (b) implementing measures to avoid excessive risks.

(c) The duty to use diligence requires that directors adopt the necessary measures for proper management and control of the company (art. 225 LSC). Without great dialectical effort, it can be inferred that, in order to adequately control a company, it will be necessary to detect and analyse the financial and non-financial risks (including operational, technological, legal, social, environmental, political and reputational) the company faces and to establish the necessary mechanisms for their management.

Regarding legal compliance and business ethics, as mentioned above, they are regarded as an indissoluble part of an adequate risk control and management policy, but beyond that:

(a) Art. 225(1) provides that "directors must hold office and discharge the duties incumbent on them under the law and under the articles of association with the diligence of an orderly businessman".

(b) Case law has recognized that directors have an "objective duty of care" that demands compliance with and observance of the rules that impinge on the company's business or sector, as well as of the duties imposed by law in relation to third parties directly affected by their actions. This can be inferred, for example, from the judgment of the Supreme Court of 23 May 2014 (RJ 2014\2943).

(c) For its part, the Attorney General's Office's Rules Instrument 1/2016[4] (affirmed by the judgment of the Supreme Court of 29 February 2016, RJ 2016\600) states that "organization and management models or corporate compliance programmes [...] are aimed at [...] fostering a true business ethics culture. The company must have a model to abide by the law in general [...]. Without a doubt, many companies have provided themselves with complete and expensive programmes with the sole aim of averting criminal accusations, but […] such programmes [must] focus on [...] reinforcing a corporate culture of respect for the law […]".

3. Risks of failing to implement effective business integrity programmes

Failure to implement effective legal compliance and risk control and management programmes could, therefore, entail liability for directors through several routes, including without limitation:

(a) *Corporate liability claim ('acción social de responsabilidad')*:

If, as a consequence of a failure to implement such programmes, penalties should be imposed on the company (criminal or otherwise), resulting in financial losses for the same

[4] *Circular 1/2016 de la Fiscalía General del Estado.*

(including those arising from reputational damage), liability could arise for the directors under art. 236 LSC from having breached the duties inherent in their position. Note that the claim can be instigated not only by the company, but also derivatively by shareholders with a certain stake and creditors in the event of inability to meet obligations as they fall due.

(b) Non-corporate liability claim ('acción individual de responsabilidad'):

According to the aforementioned judgment of the Supreme Court of 23 May 2014, "art. 241 LCS provides for non-corporate liability claims against directors when, in the discharge of their duties, they fail to comply with specific rules governing their company's business and which tend to protect the weakest, [...] [who] suffer losses directly as a consequence of such failure to comply". It should be noted that, although it is true that directors can assert, as a rule, an action for contribution against the company if ordered to compensate third parties for acts performed in the discharge of their duties, the company may plead a failure to use diligence on the part of the director as a defence.

(c) Non-application of the business judgment rule:

In order for the standard of diligence to be deemed met within the scope of the business judgment rule, art. 226 LSC requires the director, inter alia, to have sufficient information and to follow an adequate decision-making process. It seems clear, therefore, that, prior to the adoption of any strategic or business decisions, a thorough and professional analysis of the risks of such decisions must be carried out, internal control and management measures for these decisions must be established and traceability of the decision process must be ensured.

(d) Criminal responsibility

Regardless of offences for which they may be found directly responsible (for example, arts. 252, 290 et seq., and 318 of the Criminal Code [CP]), under art. 31 CP, directors may be criminally responsible for crimes committed on behalf of or on account of the company and for their own direct or indirect benefit; this holds even if the conditions, qualities or relationships that the class of offence requires to be able to be its perpetrator do not apply to the director, but do apply to the entity or person for whom or on behalf of whom such directors acted (art. 31 CP).

(e) Others:

Directors may also be held liable for a tax default (arts. 42 and 43 of the Taxation Act) or Social Security default (art. 18 of the Social Security Act) by the company, or for violations by the company of competition law (arts. 61(2) and 63(2) of the Competition Act), securities market law (arts. 306 and 307 of the Securities Market (Recast) Act), environmental law (art. 13 of the Environmental Responsibility Act 26/2007 of 23 October 23) and consumer protection law.

Conversely, business integrity programmes have additional advantages, including the prevention of claims against the company (or the possibility of relying on the same for the purposes of exculpation or mitigation, as the case may be), effective crisis management, reputational protection and improvement, and the reduction of financing or insurance costs. Hence, most respondents to the OECD survey on business integrity and corporate governance (as reported in the OECD report 'Corporate Governance and Business Integrity: A Stocktaking of Corporate Practices') characterised the resources allocated to these programmes as an investment, not an expense.

4. Requirements for the effectiveness of business integrity systems

In any case, in order to be effective, business integrity systems must meet, at the very least, the following requirements:

(*a*) *To be adapted to the risks and to the legislative fields applicable to the company*, for which it must start with a diagnosis that allows the board to know what are the risks for the company and the possible situations of non-compliance by the company.

(*b*) *To be aligned with the company's strategy and risk appetite*. This point is particularly relevant because the above-mentioned OECD report shows that the reason why many risk prevention systems had failed was because they were not compatible with the company's strategy or risk appetite.

(*c*) *To be comprehensive and coordinated*. They should be applicable to the whole company or, where appropriate, the group of companies (without disregarding, therefore, subsidiaries) and should allow coordinated action of all the areas involved.

(*d*) *To include policies or protocols for the prevention, detection and treatment of "serious corporate misconduct"*, which, as defined for the purposes of the above-mentioned OECD report, "relates to corporate conduct, whether directly or through business relationships, including in the supply chain, that violates national or international laws and regulations, including but not limited to anti-trust/competition, bribery of foreign public officials, private sector bribery, cybercrime, data protection and privacy, environment, fraud, human rights, industrial relations and labour, intellectual property, money-laundering, terrorism and proliferation-financing, product/service safety, sanctions and export controls, securities and finance, sustainability, tax and workplace safety".

(*e*) *To be promoted and supervised by the governing body*. Various international organizations, such as the OECD and the IMF, stress the importance of the board taking on a leading role in promoting business integrity systems. Business integrity systems can only be effective to the extent that the organization perceives that directors, who are at the apex of the business organization, are committed to legal compliance and rigorous risk management.

(*f*) *To have a business integrity function created*, with its powers, responsibilities and internal rules of operation clearly stated. The size and composition of this function will vary

depending on the company's characteristics, but, wherever possible, a multidisciplinary team is advised in order to integrate the different business areas and areas responsible for risks (legal, tax, financial, employment, etc.).

(g) *To be part of the internal decision-making process*. Issues related to business ethics and legal compliance should be part of the decision-making process, which may require the business integrity function to be consulted, to make recommendations or to have veto power in relation to certain decisions. In any case, a written record of any assessment made by the business integrity function would be advisable.

(h) *To be simple* or, at least, the least burdensome possible, to facilitate compliance.

(i) *To be accompanied by continuous training* of both the board and the company's managers and employees with responsibility for risk and legal compliance.

(j) *To be subject to periodic review and adaptation*.