


The COMPLIANCE function



The sheer complexity of companies nowadays and the increasingly demanding regulatory framework call for a compliance function to identify the risk of breaching legislation and advise companies of same. This article analyses the origins of this function and the underlying legislative base in Europe's insurance sector.

INTRODUCTION

The concept of risk compliance, partly due to the continuous regulatory developments that affect it, directly or indirectly, continues to evolve as an essential element of the governance system for companies. Institutions in the financial and other sectors have put into place or are introducing compliance rules programmes to manage a new risk within their global map of corporate risks: the risk arising from regulatory compliance.

Running alongside and associated with the concept of compliance risk is the definition of the compliance function. The extent of activity in respect of this function («the right thing to do»), gives rise to very varied interpretations on its content. Unlike Anglo-Saxon cultures, which have dealt with the subject for a longer time, ethical behaviour becomes the key to development, from other standpoints, greater emphasis is put on the purely regulatory aspect.

In today's world, it is impossible not to consider the regulatory field as a risk aspect and this is borne out by the continuous surveys in the financial sector, and more specifically in the insurance sector, which signal the flood of national and international regulations as one of great concern.

JUAN PABLO OLMO
MAPFRE



ILLUSTRATION STOCK

The increase in the complexity of organisations and growing scope and complexity of the regulatory environment make it especially important for companies to manage and control compliance with external (general legislation and sector regulations) and internal regulations (corporate policies, rulings on ethics and behaviour) in order to avoid economic sanctions and, more importantly, to safeguard their reputations against claims of malpractice or non-compliance with regulations. To this end, the introduction of a compliance function is justified and which should identify the risks of regulatory non-compliance, prepare assessment after risk evaluation, alert possible non-compliance, and follow-up on its correction and advise the Board on its findings and conclusions.

COMPLIANCE RISK

The broadest meaning of compliance risk is that which describes it as the risk of suffering regulatory or legal sanctions, material financial loss or loss of reputation that a company may suffer due to non-compliance with laws and other regulations, rulings and internal or external standards or administrative requirements applicable to their activity.

As opposed to *ex-post* action, which has been the traditional action scenario for legal departments i.e., a reactive response to the opening of judicial or administrative procedures that require a line of defence to be set up, the action in respect of compliance risk needs to be *ex-ante* with regard to the materialization of the risk.

These actions require two types of response. On the one hand, an advance analysis and evaluation of the repercussions that any changes in the legal environment might have on the company's operations and, on the other hand, the risk management of compliance within an organisation's overall management through the use of techniques generally developed for the management of other risks. These include the successive phases of identification, evaluation of financial impact and the probability of occurrence, implementation of mitigating measures, follow-up and dissemination and information on the process.

The approximation of compliance risk management is no way static but, rather, evolves over time. Important time-related milestones include:

- 1991. US Federal Sentencing Guidelines for Organizations.
- 1998. Australian Standard AS 3806-1998. Compliance Programs.
- 2002. Sarbanes-Oxley Act.
- 2003. Insurance Core Principles, Standards, Guidance and Assessment Methodology (IAIS).
- 2005. Basel Committee on Banking Supervision. Compliance and the compliance function in Banks.
- 2006. Directive 2006/73/CE, 10th. August, 2006 (MiFID).
- 2006. Australian Standard AS 3806-2006. Compliance Programs.
- 2007. Managing Compliance Risk in Major Investment Banks – Good Practices (FSA. UK).

- 2009. Directive 2009/138/CE, 25th. November, 2009 (Solvency II).
- 2010. Good Practice Guidance on Internal Controls, Ethics and Compliance (OCDE).
- 2011. IDW Assurance Standards 980. Principles for the Proper Performance of Reasonable Assurance Engagements Relating to Compliance Management Systems (Institut der Wirtschaftsprüfer).
- 2011. Insurance Core Principles, Standards, Guidance And Assessment Methodology (IAIS).

THE COMPLIANCE FUNCTION IN THE EUROPEAN NON-INSURANCE FINANCIAL SECTOR

In the European non-insurance financial sector, the compliance function is responsible for the implementation of procedures that ensure broad compliance with internal and external regulations. The basic norms that control such actions are the principles established by the Basel Committee on Banking Supervision and the European norms arising from Directive 2004/39/EC of the European Parliament and Council of 21st. April 2004 on markets involving financial instruments (MiFID), and Directive 2006/73/CE of the Committee of 10th. August, 2006 which applies Directive 2004/39/EC of the European Parliament and Council in respect of the organisational requisites and operating conditions for investment companies.

Basel Committee on Banking Supervision

In April of 2005, the Basel Committee on Banking Supervision made public a document with



IN THE EUROPEAN NON-INSURANCE FINANCIAL SECTOR, THE COMPLIANCE FUNCTION IS BASED ON THE PRINCIPLES ESTABLISHED BY THE BASEL COMMITTEE OF BANKING SUPERVISION AND THE EUROPEAN NORMS ARISING FROM DIRECTIVES 2004/39/CE AND 2006/73/CE.

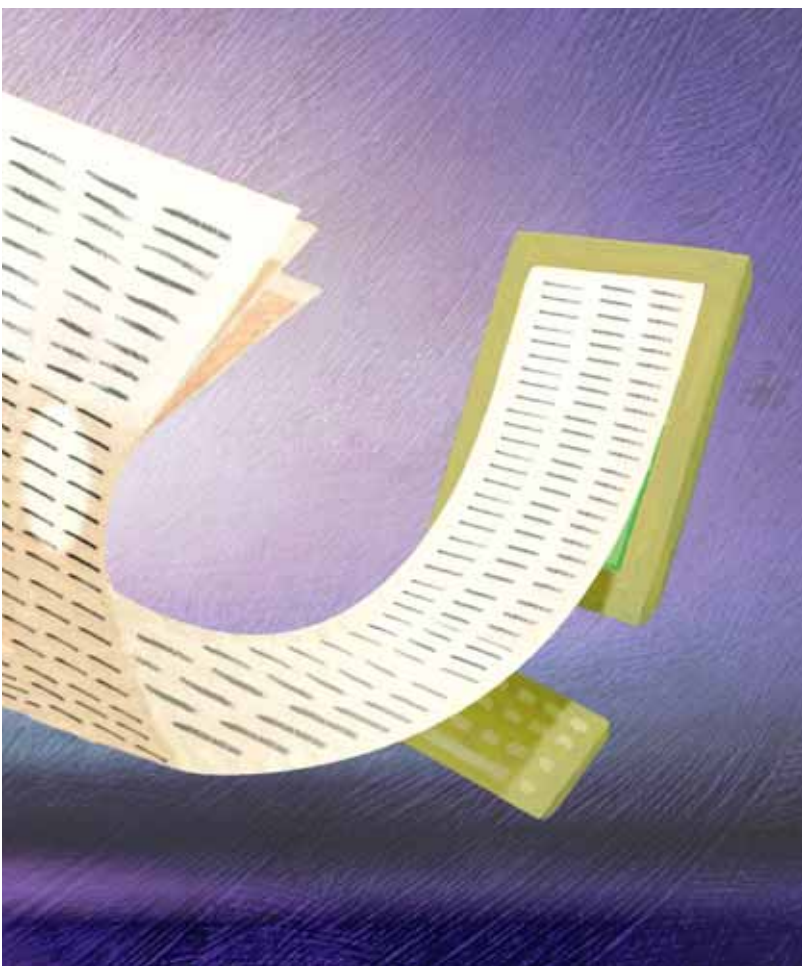
recommendations on «Compliance and the compliance function in banks», in which guidelines based on high-level principles were established for the management of compliance risk and the introduction of a compliance function in the banking sector.

The aforementioned document defines compliance risk in a similar way to that indicated above. Thus, compliance risk is defined as including both external and internal norms which are both *stricto sensu* norms and self-regulatory in nature. It also points out that it covers questions such as market conduct, the management of conflicts of interest and appropriate consumer advice. Additionally, specific subjects such as the prevention of money laundering, the finance of terrorism are dealt with, and its jurisdiction extends to fiscal

norms that are relevant in the design of products or client advice.

In the recommendations document prepared by the Basel Committee on the compliance function, the following principles should be highlighted:

- Compliance must form part of the culture of the organisation, and is solely the responsibility of specialist compliance staff.
- The Board of Directors is responsible for the supervision of compliance risk management. The Board must approve the bank's compliance policy which should include a formal document that establishes a permanent and effective function. The Board must supervise the implementation of the policy, guaranteeing that compliance problems are resolved quickly and effectively by senior management with the help of the compliance function.
- Senior management is responsible for establishing and communicating a compliance policy and for ensuring that it is observed. With the assistance of the compliance function, at least once a year, senior management should identify and evaluate the principle risks that the organisation faces and the plans for managing them. Senior management is responsible for establishing an effective and permanent compliance function within the organisation, as part of its compliance policy.
- The compliance function must be independent and sufficiently resourced and its responsibilities should be clearly specified.
- The compliance function should have a formal status within the organisation in order to give it an appropriate position, authority and independence. This may be set out in the organisation's compliance policy or in any other formal document. The document should be communicated to all staff throughout the



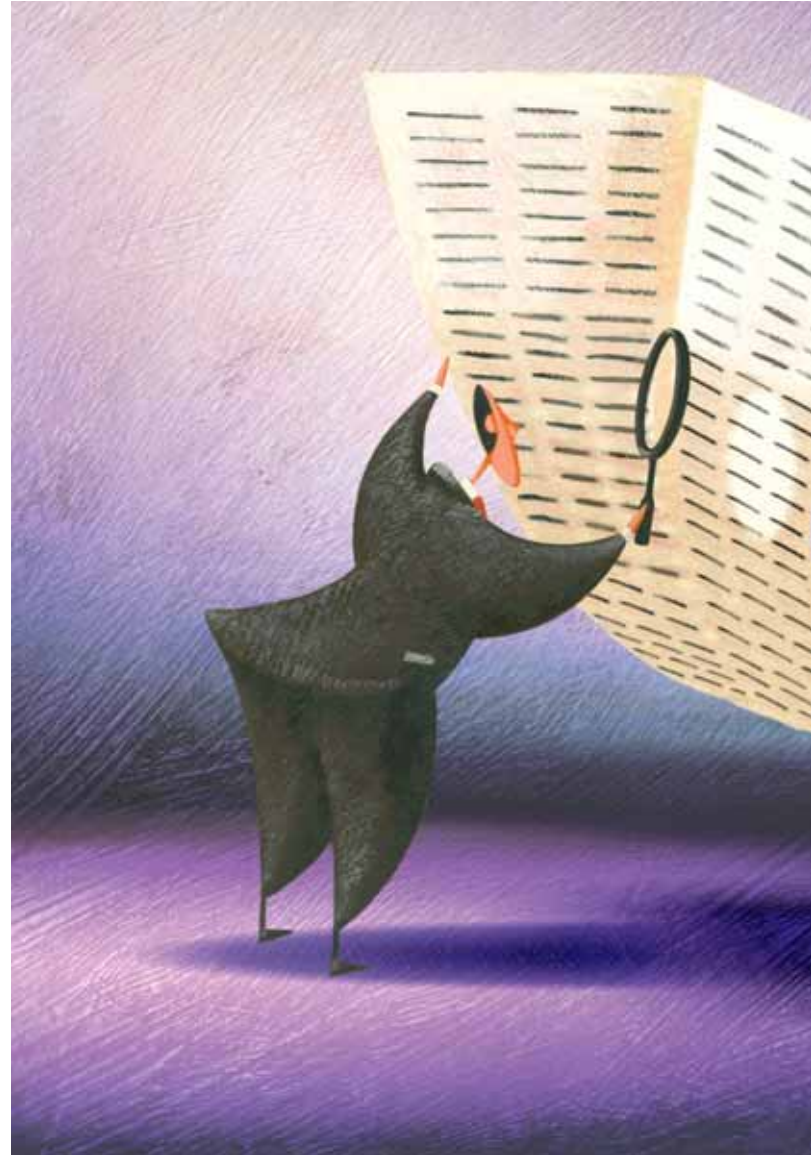
organisation and should establish: its role and responsibilities, measures to ensure its independence; its relationship with other risk management functions within the organisation and with the internal audit function; in those cases where compliance responsibilities are carried out by staff in different departments, how these responsibilities are to be allocated and limited; its right to access information necessary to do its job, and the corresponding duty of organisation staff to co-operate in this respect, its right to be able to freely express and disclose its findings to senior management, and if necessary, the Board of Directors.

■ There must be a Director of Compliance with responsibility for co-ordinating the identification and management of the organisation's compliance risk and for supervising the activities of other compliance function staff. The compliance function staff should not be in a position of potential conflict regarding their compliance responsibilities and other responsibilities, and it is preferable that they only have compliance responsibilities.

■ The organisation's compliance function should have sufficient and appropriate resources to carry out its responsibilities effectively.

■ Some of the compliance function responsibilities include:

- Advice on compliance with laws, rules and standards, including updated information on developments regarding same
- Training of staff on compliance matters.



- Identification, measurement and assessment of compliance risk.
- Monitoring, testing and reporting on the compliance risk.
- If the organisation has a new product development committee, then the compliance function staff should be represented on it.

THE 2006/73/EC DIRECTIVE ATTACHES A SIGNIFICANT ROLE TO THE COMPLIANCE FUNCTION. THIS IS REFERRED TO UNDER ARTICLE SIX, WHICH REQUIERES INVESTMENT FIRMS TO SET UP AND MAINTAIN A PERMANENT AND EFFICIENT COMPLIANCE MONITORING ORGANIZATION.

- The compliance function may have specific statutory responsibilities and it may also liaise with relevant external bodies, including regulators and external experts.
- The duties of the compliance function should be carried out under a compliance programme that sets out its planned activities.
- The compliance function must be subject to a periodical review by the internal audit function. This principle implies that the compliance function and the audit function should be separate, so as to ensure that the activities of the compliance function are subject to independent review. The division of activities between the compliance function and the internal audit function should be documented in respect of risk assessment and monitoring. The audit function should keep the compliance function informed of any audit findings relating to compliance.
- Organisations should comply with applicable laws and regulations in all jurisdictions in which they conduct business, and the organisation and structure of the compliance function and its responsibilities should be consistent with local regulatory requirements.
- The compliance function should be regarded as a core risk management activity within the organisation and, although specific tasks of the compliance function may be outsourced, they must remain subject to appropriate supervision by the compliance director.

Commission Directive 2006/73/EC of 10th. August 2006

The 2006 Directive which applies the MiFID Directive as regards organisational requirements and operating conditions for investment firms, attaches a significant role to the compliance function. This is referred to under article six which requires investment firms to set up and maintain a permanent and efficient compliance monitoring organization.

The compliance monitoring function is required to operate independently and must comply with the following requirements:

- The compliance monitoring function must have the necessary authority, resources, expertise and access to all relevant information.
- An officer responsible for compliance must be appointed.
- The relevant persons involved in the function monitoring must not be involved in the performance of services or activities that they control.
- The method of determining the remuneration of the relevant persons involved in the compliance monitoring must not compromise their objectivity, either in reality or potentially.
- The compliance monitoring organisation is assigned the following responsibilities: to monitor and, on a regular basis, to assess the adequacy and effectiveness of the measures and procedures put in place and, also, the actions taken to address any deficiencies in the firm's compliance with its obligations, to advise and assist the relevant persons responsible for carrying out investment services and activities to comply with the firm's obligations under the MiFID Directive.

THE COMPLIANCE FUNCTION IN THE EUROPEAN INSURANCE SECTOR

Legal development has been mixed within the European insurance sector since it has not been the subject of attention within the community Directives; so, whilst in Spain we do not have any provisions on the matter, one can find regulations in the United Kingdom or Italy, to cite just two examples.

Before analysing the legislation arising out of the Solvency II¹ Directive in relation to the compliance function, it is worth pointing out that the International Association of Insurance Supervisors (IAIS) in their last 2011 version under the eighth principle of their Insurance Core Principles² refers to the directives that worldwide insurance regulators should follow on questions of risk management and internal control. Under this principle, they identify, by way of recommendation, those requirements that the compliance function should comply with, and its content is very similar to that referred to above pertaining to the banking sector.

As far as Solvency II is concerned, there is little regulation with regard to the compliance function. However, in December 2010, the European supervisory authority, CEIOPS (now EIOPA: European Insurance and Occupational Pensions Authority) made public a document for consultation that contained a clearer definition on the governance system. This document was merely a draft which now must be interpreted as having been superseded by the Guidelines³ on the governance system issued by EIOPA last September. In the latter, EIOPA preferred not to establish function tasks or responsibilities on the basis that the Directive is sufficient. After confirming the key nature of the function and its important role in ensuring that the preparatory measures adopted by the company are sufficient to achieve compliance with the requirements at the beginning of Solvency II, EIOPA allows companies the freedom to

organize the compliance function and its responsibilities.

The Solvency II Directive states the following under the article dedicated to internal control:

Article 46. Internal Control.

«1. Insurance and reinsurance undertakings shall have in place an effective internal control system.

That system shall at least include administrative and accounting procedures, an internal control framework, and appropriate reporting arrangements at all levels of the undertaking and a compliance function.

2. The compliance function shall include advising the administrative, management or supervisory body on compliance with the laws, regulations and administrative provisions adopted pursuant to this Directive. It shall also include an assessment of the possible impact of any changes in the legal environment on the operations of the undertaking concerned

¹ Directive 2009/138/EC of the European Parliament and Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

² www.iaisweb.org/Insurance-Core-Principles--795

³ eiopa.europa.eu/en/consultations/consultation-papers/2013-closed-consultations/march-2013/guidelines-on-preparing-for-solvency-ii/index.html





AS FAR AS SOLVENCY II IS CONCERNED, THERE IS LITTLE REGULATION WITH REGARD TO THE COMPLIANCE FUNCTION. HOWEVER, THE EUROPEAN SUPERVISORY AUTHORITY EIOPA ALLOWS COMPANIES THE FREEDOM TO ORGANIZE THE COMPLIANCE FUNCTION AND ITS RESPONSIBILITIES

and the identification and assessment of compliance risk».

Furthermore, the draft of Delegated Regulation of the European Commission that will eventually be converted into the development of the Solvency II Directive, states that the compliance function will include a compliance policy and plan. It is expected that this policy will define the responsibilities, competencies and hierarchical lines for the function and will have to consider all of the relevant areas of the company's activity and its exposure to compliance risk. Moreover, it assigns the compliance function with the responsibility of evaluating the suitability of the measures introduced by an insurance company to prevent non-compliance.

Apart from this specific compliance function regulation, one should consider all those aspects that are regulated together for key or fundamental functions of insurers' governance systems and these should include the risk management function, the compliance function, the internal audit function and the actuarial function.

The regulation regarding these functions can be found in articles 41 and 49 of the Solvency II Directive, and in the EIOPA Guidelines on the governance system referred to above. In the future, there will also be further regulatory development through the Delegated Regulation of the European Commission. The last draft of this Regulation, dated 31st. October, 2011, includes the regulation of this function under articles 249 to 264.

The following is a brief summary of that regulation.

Companies will have to incorporate the key functions into their organizational structure in such a way as to guarantee that each function is free from influences that can compromise its independence. Each function must operate at the most senior level and report directly to the Board.

Those persons who are carrying out these tasks must be able to communicate with any person within the organisation and have access to any information that they consider to be relevant for the job. The regulation also contemplates that they should have the authority, resources, experience and qualifications to carry out their work.

In general, there are no strict guidelines for the organisation of these functions and, therefore, it is up to each company to organise them in practice and to entrust them to their own staff or outsource them, externally or within the same group.



The organization of the functions must take into account the nature, volume and complexity of the company's operations. With the exception of the internal audit function, it is expressly stated that, for smaller or less complex companies, a person or organisational unit may undertake more than one function.

In all cases, insurance companies must have, at the very least, written policies referring to the risk management, compliance and internal audit functions which must be approved by the Board. Where applicable, there should be a written policy on the outsourcing of key functions, if this is the chosen method of implementation.

All persons exercising key functions have to comply with aptitude (qualifications and experience) and integrity requirements. Moreover, companies should notify the supervisory body of the appointment of the function heads.

Article 35 of the Solvency II Directive and article 297 of the draft of the Delegated Regulation of the European Commission regulate the information to be provided to the supervisor with respect to the governance system in general and the key function in particular. At the same time, on the same matter, article 51 of the Solvency II Directive and 285 of the Delegated Regulation of the European Commission, specify the information to be published in the annual report on the financial and solvency situation, and which is publicly available.

Furthermore, it should be pointed out that article 246 of the Solvency II Directive indicates that the articles applicable to individual companies on governance systems matters are to be of *mutatis mutandis* application at group level.

Finally, the draft Ministerial Order on measures for progressive adaptation by insurance and reinsurance undertakings to the new Solvency II framework on the matter of governance systems, presented by the Insurance and Pension Fund General Directorate at the Advisory Council last September, dedicates article seven to the compliance function, with the following words:

Article 7. Compliance function.

«The compliance function will consist of advising the governing body on compliance with legal, regulatory and administrative dispositions that can affect the undertaking including compliance the company's own internal norms. It will also provide evaluation on the impact of any changes in the legal environment for the company's operations and the determination and evaluation of compliance risk.»

It can be appreciated that the wording is almost identical to that contained in the Solvency II Directive, in such a way that there are three general competencies assigned to the function:

- Advising the Governing Body.
- Evaluation of the impact of regulatory changes.
- Determination and evaluation of compliance risk.

However, there is a nuance that is worth pointing out since it affects the interpretation on the intended extent to which the function is deployed, at least concerning advising the Board. The Directive appears to limit these actions to the matters referred to in the Directive whilst the Spanish ruling expands the competency to all regulations that affect the company, including its own internal norms.



ARTICLE 35 OF THE SOLVENCY II DIRECTIVE AND ARTICLE 297 OF THE DRAFT OF THE DELEGATED REGULATION OF THE EUROPEAN COMMISSION REGULATE THE INFORMATION TO BE PROVIDED TO THE SUPERVISOR WITH RESPECT TO THE GOVERNANCE SYSTEM IN GENERAL AND THE KEY FUNCTION IN PARTICULAR.



IN CONCLUSION

Following the directives laid down by EIOPA, the compliance function should be understood to be sufficiently developed from the point of view of the ruling contained in the Directive and, therefore, it is defined as an advisory function to the Board of Directors, that carries out an anticipatory function in respect of possible non-compliance with regulations, including both internal and external regulations, regardless of whether such laws are development regulations or self-sectoral regulating codes.

At this point, before deciding arbitrarily on which subjects are outside the scope of the compliance function, it would seem more appropriate to think that it can be implemented in different departments, as a sole function, coordinated from a Compliance Unit, if you will. As we have seen, EIOPA have made it clear that it is companies themselves who should decide on how to organise the function. Therefore, the departmental division and assigning of responsibilities is not questioned by the supervisor and each organisation can guarantee compliance in accordance with their own structure.

The function has essentially a preventative nature and this is apparent in two aspects:

- The evaluation of the foreseeable effects on the organization from regulatory changes.

- The management of compliance risk in its different stages: identification of risks in the different regulations, evaluation of the probability of the risks occurring and their consequent impact, mitigation of some through the introduction of internal controls or specific policies, monitoring and reporting to the Board on the whole process.

The principles that should govern the practice of the compliance risk management function should be:

- The independence of the function in relation to business areas.
- The involvement of senior management.
- The establishment of a well-defined organisational structure with sufficient resources.
- Access to information and all functions and processes.
- A written policy, approved by the Board, which defines responsibilities, competencies and reporting obligations.
- Training that guarantees an adequate level of knowledge on applicable regulations on the part of the organisation.
- The preparation of verification and supervisory programmes developed through compliance plans.

Together with the negative financial and reputation effects arising directly from non-compliance, companies should also evaluate other aspects. The implementation of the compliance function should consider not only those aspects related to legal obligations but also take into account other benefits which the function's existence might provide as an exculpatory argument against any possible criminal allegations against the company, such as individual defence mechanisms for Board members. Perhaps, and even more importantly: the public demonstration of the organisation's commitment to general behavioural standards, generating greater confidence and enhancing its reputation. |