**РАЗДЕЛ 4**
**УГОЛОК ПРАКТИКА**

**SECTION 4**
**PRACTITIONER'S CORNER**

# COMPLIANCE RISK AND THE COMPLIANCE FUNCTION COULD ENHANCE CORPORATE GOVERNANCE NOT ONLY IN BANKS BUT IN OTHER KIND OF ORGANIZATIONS AS WELL

***Rodolfo Apreda****

***Abstract***

This paper sets forth that compliance risk and the compliance function are powerful devices to enhance corporate governance. Firstly, it reviews the contribution made to the subject by the Bank for International Settlements (BIS). Next it argues that compliance risk matters not only in financial but in any other organization. Afterwards, it deals with how the compliance function can be shaped so as to grant independence and accountability to such managerial endeavors. Later, it shows some shortcomings in the BIS' choice of governance principles. Lastly, it brings forth a set of governance principles related to compliance risk and the compliance function on behalf of financial as well as non-financial organizations.

**Keywords**: compliance risk, compliance function, accountability, corporate governance, banks governance, accountability

*Director of the Center for the Study of Private and Public Governance at the University of Cema. E-mail: ra@cema.edu.ar

## Introduction

In April 2005, the Bank for International Settlements at Basel (BIS) issued a paper under the title of *Compliance and the Compliance Function in Banks*[1].

Let us review how BIS introduces the two key notions delivered in the above-mentioned report. To start with, compliance risk comes defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities[2]. Afterwards, it introduces the expression compliance function which intends to be *staff carrying out compliance responsibilities*[3].

By no means I would contend that these notions fail to be distinctive and relevant in governance analysis. However, a certain number of questions come to my mind and the paper will attempt to find out plausible answers to each of them:

Are compliance risk and the compliance function tools to be only used for the improvement of banks' governance, or could we also profit from them when dealing with Corporate Governance issues that concern to any sort of private organization?

How would it be possible to lay foundations for the compliance function so that independence from internal auditing might be granted in practice?

[1] There was a preliminary draft issued in 2003 under the title of *The Compliance Function in Banks*, which was intended as a consultative document.

[2] As a shorthand, the Bank substitutes the expression "*compliance laws, rules and standards*" for likely settings on which failures in compliance may arise eventually.

[3] The Bank remarks that the compliance function should stem out of a set of governance principles that we are going to review later in this paper.

What kind of accountability is to be expected from this function?

To expand on these ideas and frame a coherent set of answers, we move on to meet the following agenda:

In section 1, the BIS proposal will be briefly surveyed. Afterwards, it will be for section 2 to uphold the case of compliance risk as closely related to any governance purposeful design. Section 3 will raise the problem of how compliance risk distinguishes itself from risk management. Next section will address the double-edged issue of how the compliance function can preserve its independence from the audit function, and to whom it should be held accountable.

Section 5 will show which are the principles of governance introduced by the BIS to shape compliance risk and the compliance function in financial institutions, bringing into view some distinctive shortcomings on this approach. Last of all, and in section 6, we are going to enlarge upon the impending changes the compliance function gives rise in the governance design of the organization, either financial or non-financial.

## 1. The Bis' Proposal

Failure to comply with laws, rules and standards is a likely risk that most of financial institutions run as a matter of course in their everyday activities. Any attempt to avoid or redress the consequences of such lack of compliance seems sensible, and the Basel bank's proposal comes in handy to meet this long-standing problem.

Another rationale for being concerned with compliance risk in banks, it stems from customers' illegal activities in which the bank could become involved (for instance, tax avoidance, money laundering, international terrorism activities).

On the grounds of its definition of compliance risk, the BIS sets forth a managerial function that it could discharge compliance responsibilities, making a case for giving latitude to banks on how this function should be designed and put into practice. Some banks[4] would prefer to have the compliance function as a component of the more general operational risk function, while other may split the tasks eventually.

However, and in the broadest sense, stress is laid upon independence and full measure in resource endowment. We must bear in mind that the underlying governance assumed by BIS consists of a Board of Directors and Senior Management, or their equivalent counterparts when dealing with different institutional backgrounds.

Finally, the BIS's paper expands on responsibilities of the Board of Directors and the Management, as well as a collection of principles that should guide the compliance function.

## 2. Compliance Risk also Matters in Corporate Governance

If we move on to the private realm, where any sort of organizations meet together in their transactional environments and are subject to similarly complex networks of stakeholders, we must ask ourselves whether compliance risk has any further relevance for those organizations which convey a non-financial nature.

Let us summon again the BIS's definition of compliance risk:

*the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities*

Surely, the gist of this definition is preserved if we proceed to reframe it this way:

*compliance risk is about assessing and preventing the risk of sanctions, material loss of any kind, or loss to reputation an organization may suffer as a result of its failure to comply with the constraints of its institutional environment.*

It is noteworthy that laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its activities, all of them actually pertain to the institutional environment within which any organization strives towards the fulfillment of its goals[5].

But such environment is much more variegated for non-financial enterprises, including features like conventions, international regimes, gatekeepers monitoring and punishing, as well as environmental damages.

We have to bear in mind that the financial system is very special, and strongly regulated in each country, and whose main consequence amounts to a far more regulated governance than in the non-financial sector where we surely find out broader degrees of self-governance. Hence, it becomes apparent that compliance risk does actually matter in corporate governance, whatever the kind of organization we are interested in.

## 3. Compliance Risk and Risk Management

Once we lend credence to compliance risk as a suitable subject in governance studies, we must give heed to the following issue:

How does compliance risk become distinctive and separate from risk management in general, and

[4] The BIS's proposal covers ordinary banks, banking groups, even holding companies whose subsidiaries are dominated by banks.

[5] By institutions, it will be meant throughout this paper and following Douglas North (1990), "the rules of the game in a society or, more formally, (they) are the humanly devised constraints that shape human interaction".

from the tasks other centers in the organization carry out to prevent their specific risks?

Almost every operation undertaken at any center within a modern organization meets with risk exposure. We are going to highlight some types of risk that commit surveillance, prevention and expenses from any company, in contradistinction with core problems addressed by the concept of compliance risk. The classification is only didactic and by no means intends to be complete.

## Production, administrative, and distributional centers

Usually, these centers run manifold risks for which companies arrange to purchase insurance. There are many kinds of insurance contracts, among which we can notice accident (that covers theft and a wide range of liability risk), property and liability insurance (multiple-line coverage except life and fire insurance), engineering risks, fidelity (against breach of contract and dishonesty losses), life and fire insurance, marine insurance, labor accidents and health insurance, goods-in-transit insurance, weather and lighting insurance, even political insurance.

Closely related to governance issues are contracts companies take out to cover their Directors and Managers from liability actions from third parts. Besides, in developing countries, it is customary to buy insurance on risks of kidnapping, or to prevent political disruptions like property forfeiture and populist-socialist measures intended to grab companies' assets or earnings.

## Trading risks

When any company gets access to inputs or sell outputs there are risks that stem from market transactions. Therefore, organizations must curb their risky positions with instruments other than insurance policies. Such trading environments call for the so-called "derivatives markets", through the use of futures and forwards contracts, options, swaps and, in general, arrangements of these elementary financial instruments to tailor up highly complex and distinctive "combos" to shield companies from risk.

Among the main types of risk that arise out of trading and current operations, we can highlight the following ones:

- ✓ commodity prices;
- ✓ interest rates;
- ✓ financial assets prices;
- ✓ exchange rates;
- ✓ systemic risk from particular financial markets.

Therefore, and from the foregoing remarks a) and b), we can lastly assert that any company crossing a natural threshold of size, scope and scale for its operations, it must regard risk as a costly hurdle to be accounted for. And this commitmen proceeds firstly by means of an active involvement at each center bearing risk exposure and, secondly, by setting up a managerial function to cope with risk problems. The foregoing discussion shows that the governance of any organization has to make provision of how to design a safety net for risk exposure. Failure in addressing this topic may impair the pursuit of growth, value creation, and the manifold purposes conveyed in the foundational charter. It is our contention that the management of compliance risk would be likely contested most of the time either from the Auditor's Office or the head of the Risk Management Center.

This could be prevented when such management is regarded as an endeavor with unequivocal focus. Exhibit 1 conveys internal and external control linkages that arise out of the control system of big organizations within which a compliance function does matter eventually.

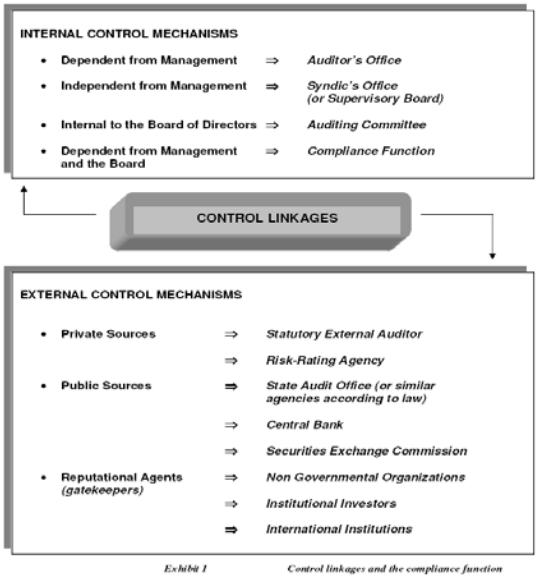


*Exhibit 1* *Control linkages and the compliance function*

For compliance risk to become a self-contained notion, it should match the following claims:

*topic:* could we tell what this concept is about?

*scope:* does it have a specific scope of problems to deal with?

*distinctiveness:* can a compliance center map out its features and goals in different ways as similar other centers do eventually?

In connection with the first demand, we set forth in section 2 a modified definition of compliance risk, which seems worthy of being recalled here:

*compliance risk is about assessing and preventing the risk of sanctions, material loss of any kind, or loss to reputation an organization may suffer as a result of its failure to comply with the constraints of its institutional environment.*

To put this another way, compliance risk deals with the hazards arising out of the manifold

institutional constraints any company must comply with.

The definition also sheds light on the second question. In actual fact, compliance risk does pertain neither to expected hazards conveyed by production, administrative and distributional centers, nor the wide-ranging scope of trading risks.

Turning back to the third question and giving heed to the Auditor's tasks, it will be apparent that most of them fall under the guise of an *ex post* approach of compliance duties, at least from a clinical viewpoint[6] intending to find out and redress oversights, mistakes, wrongdoings or misrepresentations. Therefore, this function becomes mainly intertwined with financial statements, accountancy procedures, auditing benchmarks, and a complex set of duties and targets lay down in the definition of the auditing function.

In contradistinction to the Auditor's job, the approach of the compliance risk and its underlying managerial function should be regarded mostly as *ex ante* based. Hence, the clinical viewpoint for the compliance function focuses on the prevention of mistakes or failures in compliance matters, as well as the extent to which the company will exhibit responsiveness towards manifold institutional constraints.

## 4. Independence of the Compliance Function from the Auditor's Office

The compliance function seems to be an innovative managerial function, but it raises at least two daunting queries:

Provided that this function widely overlaps with the audit and the risk-management function, would it be worth setting a new function instead of allowing the latter to comprise the task and responsibility claimed by the newcomer?

To what extent does the compliance function keep itself independent of the auditing function, even of the risk management function?

A first step to discuss both queries consists in finding out whether the complexity of the organization bears the expense of building up any kind of risk management center or a full-fledged audit department. It seems likely that if we were the owners of a corner shop in the neighborhood, such an organizational design would be ruled out since it could be so expensive as to impair the minimal earnings from day-to-day transactions that grant the survival of any convenience store.

As for companies that already have an audit function, framing up compliance functions does not seem out of place although cost-benefit analysis and regulatory constraints should have the last word in this issue.

Otherwise, the auditor will carry out the compliance function as a matter of course. All in all, it is for size, scope and scale to have the last word on this issue. Exhibit 2 shows connections among lines of accountability, regular consultation among centers, and shared information in a full-fledged organization.

If we now draw our attention to the matter of how independence may become an in-built feature of the compliance function, we are going to stress three further qualifications:

To all intents and purposes, the compliance function should fall under the scope of the Internal Audit Center, like any other staff center.

However, many key topics in which the compliance function becomes involved must be directly reported the CEO's office, and not the Auditor's office.

But if the compliance function were constrained so tightly, it would not be truly independent. So, the new function should be allowed to directly report to the Board of Directors, which can be accomplished by means of a provision in the statute ruling this function, of exempting the internal accountability line whenever is regarded necessary by the compliance function head office.

On such hierarchy of accountability lines the Basel's proposal lacks of precision. In point of fact, the BIS' paper provides with some weaker, even faulty, procedures to build up the compliance function. For instance, letting the function to meet its job within another staff center, which would entail an almost fatal conflict of interest in the end. A clear-cut criterion for measuring to what extent we are able to grant independence can successfully be shaped only when we state to whom the staff function should be held accountable.

Provided the governance of any organization reaches and overpass a threshold of complexity, and the Board of Directors sets up a compliance function, never should they relinquish their ultimate control upon this function.

[6] The expression *clinical approach* is far from being used here as a metaphor only; in fact, it has been proved itself widely helpful in organization theory. As Pranger (1965) put it: "*not only does the clinician [viewpoint] accepts the total, dynamic organization as his subject matter, passively seeing and listening, rather than actively manipulating, but also becomes absorbed in its problems as the subject for inquiry.*"

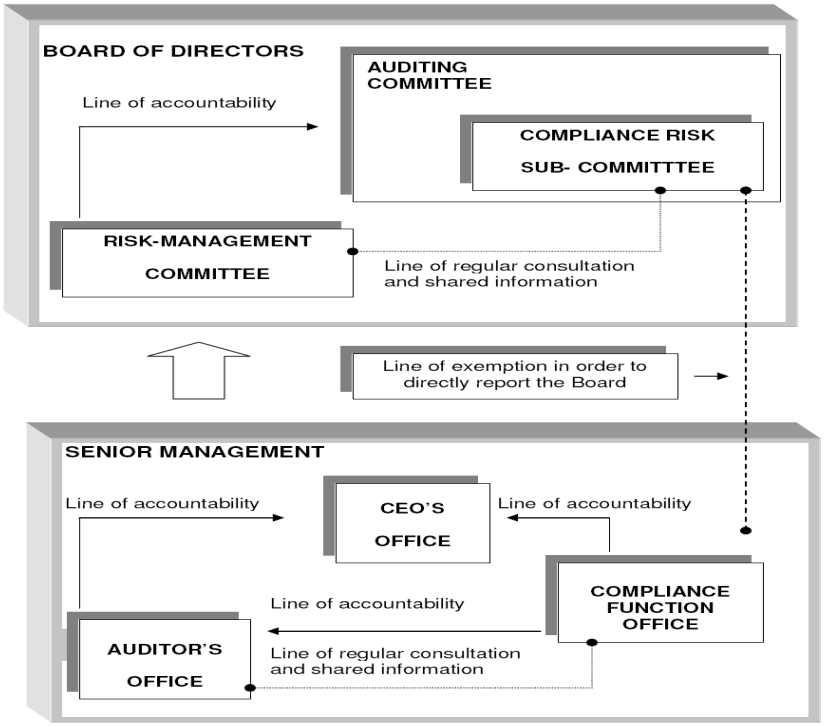


*Exhibit 2* *Lines of accountability, regular consultations and shared information, and the line of exemption granted to the compliance function office to report directly the Board of Directors.*

## 5. Basel principles of Governance for Compliance Risk and the Compliance Function

In the Basel's proposal, new principles of governance are predicated for healthy foundations of compliance risk and the compliance function.

### a) Principles concerning compliance risk

From the four principles devoted to compliance risk, we highlight the following features:

Firstly, it makes de Board of Directors in any bank responsible for managing compliance risk, approving the compliance function statute, designing a compliance risk policy, and assessing how well the bank is performing on this issue for at least once a year.

Secondly, it delegates the working of the compliance risk policy to Senior Management, which will be held on this regard fully accountable to the Board.

At this juncture, we can't help remarking that there are too many principles and they overlap too much. In point of fact, it is a sound methodology (as we are going to develop in next section) that principles should be enabling, the fewer of them the better, and they must not be mixed with good practices.

### b) Principles concerning the compliance function

Four principles are put forth in the proposal, and it seems to us some of their contents are in excess. We are going to lay stress on two of them.

Principle 4: *The Management is responsible for establishing a permanent and effective compliance function within the bank as part of the bank's compliance function.*

Afterwards, Principle 5 says that the compliance function should be independent. The Bank for International Settlements at Basel expands on this principle, qualifying independence by the fulfillment of four requirements:

- ✓ formal status within the bank;
- ✓ the function must have a compliance head;
- ✓ the function should not be placed wherever conflict of interests may arise;
- ✓ the function must be suitably staffed and any other center in the bank must give full access to information needed for the staff of the compliance function to discharge their duties.

Yet true as such requirements are bound to be, they do not touch the heart of the matter. In our opinion, the contents of this principle turn out to be misplaced. It is the case that for any managerial function three things should not be discussed: staff

and resources provision, nomination of a head, and formal status within the organization. So, it seems that the only characteristic worthy of being noticed is the one that prevents the function from being located wherever conflicts of interests may arise, albeit for most managerial cases this should also be predicated as a matter of course. Hence, it is my contention that the truly relevant feature that grants independence to the compliance function should be rooted in matching both accountability and exemption lines by means of a principle of governance, as it is displayed in Exhibit 2. This is an issue that will be taken into account in next section.

## 6. Principles of Governance for Compliance Riske and the Compliance Function: the General Case

Taking advantage of the foregoing discussion, it's time for dealing with a minimal set of governance principles to give account and constrain the exercise of an internal compliance function not only in financial but also in non-financial organizations.

We have to bear in mind, however, that for this function to be embedded into an organization, a threshold of size, scope and complexity should be assumed. Otherwise, compliance risk might become a task more easily undertaken by the internal audit office. As regards the issue of which principles should qualify to be included in a minimal list, this becomes an open-ended question. Albeit there is a wide range of options, both empirical evidence and academic spadework point to the suitability of meeting some criteria to grant coherence to the final choice:

a) Principles should be enabling.
b) The fewer, the better.
c) Principles must not be mixed with good practices.

Let us handle each of these criteria in turn.

As for principles to be enabling, this means that they give organizations latitude to do things without hindering either its inner workings or stated goals.

The natural contention about the number of principles has to do with pragmatism, but also with the fact that principles are benchmarks that lay down guidelines for prudential decision-making. Do not forget that the Founding Fathers needed only seven articles to set up the Constitution that still rules the United States.

The third issue is a thorny one. Although we have dealt with it elsewhere[7], it's worth recalling here what I meant by a Code of Good Practices:

By a Good Practices Code we mean any set of rules of behavior that allow a distinctive governance structure to be put into practice and held accountable, provided that such rules meet the following constraints:

- ✓ by necessity, they stem from the underlying governance structure;
- ✓ they match the institutional framework within which the organization not only lives and develops, but also abides by the law;
- ✓ they are in agreement with the organization's Charter and by-laws;
- ✓ and last but not least, they should become fully operational: the rules are set up within a framework that allows monitoring, assessment, updating and improvement.

Hence, one thing is a principle of governance, quite another a good practice. For each good practice we should track down its actual foundation on some matching governance's principle. The latter involves a precept, the former makes it a real accomplishment, a course of action.

Exhibit 3 briefs and highlights the minimal list of governance principles set forth by this paper, as alternative guidelines for any organization, financial or non-financial.

Two remarks about the minimal list, so as to make a distinction with the similar ones in the BIS' proposal. 1. Accountability is dealt with in Principle 3, and its scope narrowed to compliance risk. 2. Independence of the compliance function is handled by Principle 5, which includes the lines of accountability and the statutory exemption.

## Conclusions

The proposal of the Bank for International Settlements about compliance risk and the compliance function seems a sensible starting point in pursuit of improving corporate governance in financial institutions. However, it seems that should be sharpened up, mainly on issues regarding independence and accountability. The main contributions of this paper can be stated as follows:

a) It laid foundations on how compliance risk matters in corporate governance.
b) It has shown that compliance risk and the compliance function are governance drivers not only of financial but also non-financial organizations.
c) It has brought into a sharper view that independence and accountability are at the core of these governance devices, and has put forth two distinctive governance principles:
   - ✓ One for compliance risk, ruling that the CEO and the senior management are accountable for carrying out the compliance risk policy.

Another one for independence of the compliance function, which is also given exemption lines to match ist tasks with deep-rooted fiduciary duties the Board of Directors must comply with at the end of the day.

[7] Rodolfo Apreda, *The Semantics of Governance* (2005). Corporate Ownership and Control, volume 3, issue 2, pp. 45-53.

**Principle 1** **On compliance risk**

*Compliance risk is about assessing and preventing the risk of sanctions, material loss of any kind, or loss to reputation an organization may suffer as a result of its failure to comply with the constraints of its institutional environment.*

**Principle 2** **On the compliance policy**

*The Board of Directors must request from the Senior Management, or a qualified external source, to draw out the company's compliance risk policy as well as mechanisms to make it enforceable.*

**Principle 3** **Accountability**

*It is for the Senior Management to be held accountable to the Board of Directors for the fulfillment of the compliance risk policy.*

**Principle 4** **On the compliance function**

*In order that the compliance risk policy could be enacted, run and enforced, the Senior Management must set up the compliance managerial function.*

**Principle 5** **About the compliance function independence**

*For the compliance function to be independent from any other center three requirements should be met:*

- *It is held accountable only to the Internal Audit Office and the CEO's office.*
- *The head of the compliance function office is granted a statutory exemption from reporting to the CEO's office so that it could directly report the Board of Directors or its the Auditing Committee.*
- *The compliance function center must get unlimited access to any information regarded as relevant to meet its duties, from any other center in the company.*

*Exhibit 3* *A minimal set of principles of governance for compliance risk and the compliance function.*

## References


1. Apreda, R. (forthcoming in 2007) *Introduccion al estudio del Corporate Governance (La gobernancia del sector privado).* Editorial La Ley, Buenos Aires (in Spanish).
2. Apreda, R. (2005) *The Semantics of Governance: The Common Thread Running Through Corporate, Public, and Global Governance*. Corporate Ownership and Control, volume 3, Issue 2, pp. 45-53 (downloadable from the author's web page: www.cema.edu.ar/u/ra).
3. Apreda, R. (2005) *Mercado de Capitales, Administración de Portafolios y Corporate Governance*. Editorial La Ley, Buenos Aires (in Spanish).
4. Apreda, R. (2003) The Semantics of Governance. University of Cema, Working Paper Series, number 245 (downloadable from www.cema.edu.ar/ publicaciones).
5. Bank for International Settlements (BIS, Basel, 2005) *Compliance and the Compliance Function in Banks.* Basel Committee on Banking Supervision (downloadable from www.bis.org )
6. Bank for International Settlements (BIS, Basel, 2003) *The Compliance Function in Banks.* Basel Committee on Banking Supervision (downloadable from www.bis.org )
7. Bank for International Settlements (BIS, Basel, 2002) *Internal Audit in Banks and the Supervisor's Relationship with Auditors: A Survey.* Basel Committee on Banking Supervision (downloadable from www.bis.org )
8. Bank for International Settlements (BIS, Basel, 2001) *Internal Audit in Banks and the Supervisor's Relationship with Auditors.* Basel Committee on Banking Supervision (downloadable from www.bis.org )
9. Pranger, R. (1965) *The Clinical Approach to Organization Theory*. Midwest Journal of Political Science, volume 9, number 3, pp. 215/234 (downloadable from www.jstor.org/).