GLOBAL riskupdate
The quarterly independent risk review for banks and financial institutions worldwide
Q4 2014

Financial Crime Compliance:

A Brief Guide for Senior Bank Management, Compliance Officers and Internal Auditors

Also in this issue

- HR & Risk Management
- Derivatives: Limiting Market Change
- NEW BIS Bank Corporate Guidelines
- The Implications of Climate Change
- Client Money: Don't Be in a Bad Place
- The Value and Management of Intellectual Property, Intangible Assets and Goodwill
- MoneyScience Interviews Dennis Cox

NEW BIS Bank Corporate Governance Guidelines: Insights and Analysis

Risk Reward Group CEO Dennis Cox, BSc FCA CFSI, is a global banker, Big Four chartered accountant, risk management and bank internal audit specialist, as well as an international lecturer and noted published author. As an official Observer to the African Development Bank, Chairman Emeritus of the Risk Forum within the Chartered Institute of Securities and Investments (UK), former National Council Member of the ICAEW (UK) he is regularly asked to present positions and replies on behalf of financial services professional bodies to the Bank for International Settlements (BIS). In this article he offers insights and analysis on the latest BIS consultative paper on Corporate Governance for banks.

Corporate governance has been a prime concern for regulators and stakeholders since the start of the financial crisis. In response we have seen a range of pronouncements and revised sound practices papers seeking to change the way that banks operate. Now the Bank for International Settlements (BIS) has published new Corporate Governance guidelines as a consultative paper for response by 9 January 2015.

There are a number of issues that are interesting about the BIS paper in addition to the Principles that have been set out (a lucky? 13). The first is that the paper starts with a **glossary** that actually defines concepts such as Control Functions, Risk Appetite and Corporate Governance:

Control Functions
The first definition that is of interest is what they are referring to as Control Functions, which are defined as follows:

"Those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the risk management function, the compliance function and the internal audit function."

It is perhaps interesting that they have highlighted risk management and compliance and actually not mentioned internal control or ownership of the second line of defence. Risk management and the Chief Risk Officer are generally decision-making functions and therefore part of management so it is questionable the extent to which they can be seen as truly independent.

Likewise does compliance really provide the objective assessment, reporting and/or assurance that is suggested here? In many cases this may not really be the case. Clearly responsibility for compliance lies with the first line of defence and it is perhaps unrealistic to expect compliance functions to meet this objective. Indeed they should work with the business to find methods to comply with rules and regulations and therefore are unlikely to be fully independent.

That leaves internal audit, but they cannot really be a control function. Rather they bring periodic independent assessment to the Board and therefore to the Audit Committee as a committee of the Board.

Risk Appetite
Another definition worthy of consideration is risk appetite which is defined in the BIS paper as follows:

" The aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan. "

We use the following general definition:

"The level of divergence from goals and missions which are unacceptable to the Board"

However the definition provided by the BIS is clearly workable and the important thing here is the wording "decided in advance and within its risk capacity". The risk capacity is defined as "The maximum amount of risk a bank is able to assume given its capital base, risk management and control measures, as well as its regulatory constraints." Essentially this therefore links directly into the reverse stress test and the recovery and resolution plan. Within that capacity risk appetite as defined here is the level of risk that the Board are willing to accept and this clearly has a boundary at risk capacity. It is suggested that no firm should have a risk appetite that is higher than 70% of the risk capacity as defined in these terms.

Within the paper itself there is a discussion as to what a risk appetite statement really is with the following clarification as to what it should include:

"The [statement] should:

- Include both quantitative and qualitative considerations;
- Establish the individual and aggregate level and types of risk that the bank is willing to assume in advance of and in order to achieve its business activities within its risk capacity;
- Define the boundaries and business considerations in accordance with which the bank is expected to operate when pursuing the business strategy; and
- Communicate the board's risk appetite effectively throughout the bank, linking it to daily operational decision-making and establishing the means to raise risk issues and strategic concerns across the bank."

Given this definition of risk appetite and capacity that has been made this is seen as being potentially unhelpful because it brings in qualitative and quantitative measures. As capacity and appetite are both clearly values then it is necessary to change all of these measures into values. Not doing so would surely prevent appropriate risk correlation to take place. And note the alignment of risk appetite to the strategy of the bank. Risk management is not just about preventing losses; rather it is about ensuring that the goals of the bank are achieved within stakeholder expectations.

Corporate Governance

Corporate governance is an often discussed term but this new BIS consultative paper seeks to provide a definition. It states that:

"Corporate governance determines the allocation of authority and responsibilities by which the business and affairs of a bank are carried out by its board and senior management, including how they:

- Set the bank's strategy and objectives;
- Select and oversee personnel;
- Operate the bank's business on a day-to-day basis;
- Protect the interests of depositors, meet shareholder obligations, and take into account the interests of other recognised stakeholders;
- Align corporate culture, corporate activities and behaviour with the expectation that the bank will operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations; and
- Establish control functions."

Risk management is not just about preventing losses; rather it is about ensuring that the goals of the bank are achieved within stakeholder expectations.

This raises the issue of corporate behaviour which is aligned to ethical standards stated as acting with integrity. The requirement to act in a safe and sound manner means operating above the minimum standards set by regulators. They remain a minimum but not a benchmark and need to be exceeded to meet these requirements.

The New BIS Principles: Insight & Analysis

Principle 1: The Bank Board's overall responsibilities
The board has overall responsibility for the bank, including approving and overseeing the implementation of the bank's strategic objectives, governance framework and corporate culture. The board is also responsible for providing oversight of senior management.

NEW BIS Bank Corporate Governance Guidelines: Insights and Analysis

The paper discusses the **duty of care** and what they refer to as a **duty of loyalty** which they apply to the bank (of course this really means to relevant stakeholders.) To achieve this "Accordingly, the board should:

- Establish and monitor the bank's business objectives and strategy;
- Establish the bank's corporate culture and values;
- Oversee implementation of the appropriate governance framework;
- Develop, along with senior management and the CRO, the bank's risk appetite, taking into account the competitive and regulatory landscape, long-term interests, exposure to risk and the ability to manage risk effectively;
- Monitor the bank's adherence to the risk appetite statement, risk policy and risk limits;
- Approve and oversee the implementation of the bank's capital adequacy assessment process, capital and liquidity plans, compliance policies and obligations, and the internal control system;
- Approve the selection and oversee the performance of senior management; and
- Oversee the design and operation of the bank's compensation system, and monitor and review the system to ensure that it is aligned with the bank's desired risk culture and risk appetite."

Notice the level of concentration on risk appetite within this principle highlighting its importance, a trend we have seen in other papers. By trying to deal with it at this level the monitoring that needs to be conducted by the Board is enhanced. Periodic internal audit is surely not sufficiently regular to achieve this for the Board and accordingly they will need to have a structure of reporting metrics which they are able to monitor to achieve these goals.

The background to the principle continues with the following important statement on the role of the Board: **"In order to promote a sound corporate culture, the board should take the lead in establishing the "tone at the top"** by:

- Setting and adhering to corporate values for itself, senior management and other employees that create expectations that all business should be conducted in a legal and ethical manner;
- Promoting risk awareness within a strong risk culture, conveying the board's expectation that it does not support excessive risk-taking and that all employees are responsible for helping ensure that the bank operates within the agreed risk appetite and risk limits;
- Ensuring that appropriate steps are taken to communicate throughout the bank the corporate values, professional standards or codes of conduct it sets, together with supporting policies; and
- Ensuring that employees, including senior management, are aware that appropriate disciplinary or other actions will follow unacceptable behaviours and transgressions. "

So the Board needs to be seen to be doing the right things and minimising excessive risk taking. Risk management is not about not taking risks; it is about taking appropriate risks aligned to the risk appetite of the firm. Risk is the real currency of banking but imprudent risks are now clearly unacceptable and are to be avoided.

Corporate Values

There is also a discussion regarding this important topic. Changing corporate culture and developing values is never easy and the paper proposes the following to deal with this matter:

"The bank's corporate values should recognise the critical importance of timely and frank discussion and escalation of problems to higher levels within the organisation.

- Employees should be encouraged and able to communicate, confidentially and without the risk of reprisal, legitimate concerns about illegal, unethical or questionable practices. This can be facilitated through a well communicated policy and adequate procedures and processes, consistent with national law, which allow employees to communicate material and bona fide concerns and observations of any violations in a confidential way (e.g. whistle blower policy). This includes communicating material concerns to the bank's supervisor.
- There should be direct or indirect communications to the board (e.g. through an independent audit or compliance process or through an ombudsman independent of the internal "chain of command").
- The board should determine how and by whom legitimate concerns shall be investigated and addressed by an objective independent internal or external body, senior management and/or the board itself. "

Notice this is bringing the Board directly into the process for dealing with inappropriate conduct. The use of the term ombudsman is also interesting since it suggests almost a judicial process of independence which most likely does not exist in many firms. Clearly the goal is effective and open communication of key issues related to ethical standards and this is to be encouraged.

Principle 2: Board qualifications and composition
Board members should be and remain qualified, individually and collectively, for their positions. They should understand their oversight and corporate governance role and be able to exercise sound, objective judgment about the affairs of the bank.

This is further clarified with the following explanation:

"Board members should have a range of knowledge and experience in relevant areas and have varied backgrounds to promote diversity of views. Relevant areas of competence include financial and capital markets, financial analysis, financial stability, strategic planning, risk management, compensation, regulation, corporate governance and management skills."

What is clearly needed is for Boards to assess the extent to which the skills needed to achieve these goals are met by the existing board membership. We would, for example, recommend that a non -executive risk specialist be added to the Board and indeed provide such people. We also undertake training to enhance Board skills in key areas which also is important.

Too often the recruitment process within banks has not taken full account of ensuring that the necessary balance exists on a Board. This clearly now becomes of increasing importance.

Principle 3: The Bank Board's own structure and practices
The board should define appropriate governance structures and practices for its own work, and put in place the means for such practices to be followed and periodically reviewed for ongoing effectiveness.

One of the key issues is the role played by the internal audit function.

The explanation discusses the periodic review of Board performance and the role of chairs of committees, for example. One of the key issues is the role played by the internal audit function. Reviewing internal governance processes is clearly important yet difficult for the internal audit function to undertake them. The risk for the internal auditors is that they may be producing what might best be called 'career limiting' audit findings. Sometimes delegated to third-party internal audits governance audits and the findings have generally resulted in changes to structures, roles and memberships. (On one notable occasion the findings report resulted in that the entire Board resigned.) The role is important and needs to be undertaken carefully and with strategic outcomes planned for.
This section also highlights that the **financial reporting process** is a key responsibility of the audit committee, replicating the comments in the revised BIS paper on internal audit in banks. However in looking at the risk committee the following is shown:

"The risk committee of the board:

- Is required for systemically important banks. For banks of large size, risk profile or complexity it is strongly advised. For other banks it remains strongly recommended.
- Should be distinct from the audit committee, but may have other related tasks, such as finance.
- Should have a chair who is an independent director and not the chair of the board, or any other committee.
- Should include a majority of members who are independent.
- Should include members who have experience in risk management issues and practices.
- Should discuss all risk strategies on both an aggregated basis and by type of risk and make recommendations to the board thereon, and on the risk appetite.
- Is required to review the bank's risk policies at least annually.
- Should oversee that management has in place processes to ensure the bank's adherence to the approved risk policies. "

risk is the currency of the firm

What is new here is the **requirement for the members to mostly be independent directors and for the Chair to also be independent.** This is an extension to existing guidance and follows the logic of the internal audit

committee being made up of independent members. However there is clearly a difference. The risk committee within its area of responsibility does look at key limits and is part of the executive management team. It designs limits and structures aligned to the goals and missions of the firm being as interested in making money as preventing the firm from losing money. While it is agreed that some external input can improve the quality of the debate at such a committee, risk is the currency of the firm and therefore the majority of this committee should in our opinion be executive.

Principle 4: Senior management
Under the direction and oversight of the board, senior management should carry out and manage the bank's activities in a manner consistent with the business strategy, risk appetite, incentive compensation and other policies approved by the board.

There is nothing new in this area of guidance.

Principle 5: Governance of group structures
In a group structure, the board of the parent company has the overall responsibility for the group and for ensuring that there is a clear governance framework appropriate to the structure, business and risks of the group and its entities. The board and senior management should know and understand the bank's operational structure and the risks that it poses.

Again this is hardly surprising. However there is some important information in the key clarification statement provided:

"In order to fulfil its responsibilities, the board of the parent company should:

- Establish a group structure (including the legal entity and business structure) and a governance framework with clearly defined roles and responsibilities, including those at the parent company level and those at the subsidiary level;
- Define an appropriate subsidiary board and management structure to contribute to the effective oversight of businesses and subsidiaries, which takes into account the different risks to which the group, its businesses and its subsidiaries are exposed;
- Assess whether the group's corporate governance framework includes adequate policies, processes and controls and addresses risks across the business and legal entity structures;
- Ensure the group's corporate governance framework includes appropriate processes and controls to identify and address potential intragroup conflicts of interest, such as those arising from intragroup transactions;
- Approve policies and clear strategies for establishing new structures and legal entities, and ensure that they are consistent with the policies and interests of the group;
- Assess whether there are effective systems in place to facilitate the exchange of information among the various entities, to manage the risks of the separate entities as well as of the group as a whole, and to ensure effective supervision of the group;
- Have sufficient resources to monitor compliance of subsidiaries with all applicable legal, regulatory and governance requirements; and
- Maintain an effective relationship with both the home regulator and, through the subsidiary board or direct contact, with the regulators of all subsidiaries. "

Nothing here is revolutionary but it certainly is evolutionary. The most important sentence here is that the Board should monitor local compliance. That is quite a challenge. The existing structure of compliance will need to be enhanced to achieve this perhaps with internal audit also changing their role. However to get internal audit to understand local regulation in sufficient detail to undertake this role will also require training and some changes to the nature of their personnel.

Principle 6: Risk management
Banks should have an effective independent risk management function, under the direction of a Chief Risk Officer (CRO), with sufficient stature, independence, resources and access to the board.

This section is a reiteration of the existing requirements.

Principle 7: Risk identification, monitoring and controlling
Risks should be identified, monitored and controlled on an ongoing bank-wide and individual entity basis. The sophistication of the bank's risk management and internal control infrastructure should keep pace with changes to the bank's risk profile, to the external risk landscape and in industry practice.

The important point again to notice here is the emphasis on the entity basis. The obligations of entity Board directors should be enhanced to meet these requirements.

The paper does in some ways duplicate the sound practices papers including the one on stress testing, which is perhaps surprising. However there is little here which is actually new.

The remaining principles are as follows:

Principle 8: Risk communication
An effective risk governance framework requires robust communication within the bank about risk, both across the organisation and through reporting to the board and senior management.

Principle 9: Compliance
The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should approve the bank's compliance approach and policies, including the establishment of a permanent compliance function.

Principle 10: Internal audit
The internal audit function provides independent

assurance to the board and supports board and senior management in promoting an effective governance process and the long-term soundness of the bank. The internal audit function should have a clear mandate, be accountable to the board, be independent of the audited activities and have sufficient standing, skills, resources and authority within the bank.

Principle 11: Compensation
The bank's compensation structure should be effectively aligned with sound risk management and should promote long term health of the organisation and appropriate risk-taking behaviour.

Principle 12: Disclosure and transparency
The governance of the bank should be adequately transparent to its shareholders, depositors, other relevant stakeholders and market participants.

Principle 13: The role of supervisors
Supervisors should provide guidance for and supervise corporate governance at banks, including through comprehensive evaluations and regular interaction with boards and senior management, should require improvement and remedial action as necessary, and should share information on corporate governance with other supervisors.

Again much of this actually duplicates more detailed guidance provided within existing sound practices papers with little additional information.

What is Missing

The question perhaps is what if anything is missing. Notice that there is a lot of focus on risk appetite and risk management, together with compliance and financial reporting. What there is less focus on is the strategy and profitability of the firm leading to long term survival. In the current climate given the level of change that is currently taking place it is clear that Boards need to be forward looking not only in their risk management but also in their strategy. To an extent the paper is rather negative and this is perhaps understandable (if disappointing). However there are clear messages here which any firm should take into account.

Take away message

Whilst this is a consultative or discussion BIS paper we would not anticipate major change prior to finalisation. Hence we recommend that firms consider their governance practices against this benchmark and begin to develop a programme to deal with any gaps that are perceived to exist.

The author invites comments via email to DWC@riskrewardlimited.com

RISK REWARD
GLOBAL BANKING & FINANCIAL SERVICES EXPERTS

Risk Reward Limited

part of Risk Reward Group of Companies

Global Headquarters

Risk Reward Ltd
60 Moorgate, 1st Floor,
London EC2R 6EL
United Kingdom

Office hours: London (GMT)
09.00 – 18.00 Monday – Friday

tel: +44 (0)20 7638 5558
fax: +44 (0)20 7638 5571

Risk Reward Americas

Office hours: (EST)
09.00 – 18.00 Monday – Friday

tel: +1 (917) 310-1334 New York
+1 (305) 831-4913 Miami

email:info@riskrewardlimited.com

www.riskrewardlimited.com

designed by mfp
info@mfp.me.uk