GLOBAL riskupdate
The quarterly independent risk review for banks and financial institutions worldwide
Q1 2016

Who Will Want to be a Compliance Officer?

Also in this issue

- Trying to Improve Corporate Governance
- So Who Needs Technical Due Diligence?
- The Changing World of Political Risk
- What Happened to Risk Management?
- What is Risk Appetite?

Trying to Improve Corporate Governance

In July 2015 the Bank for International Settlements reissued its paper Corporate Governance Principles for Banks (paper d328). This sets out the various principles that banks need to cover. As always there is a lot in a BIS paper so in this article Global Risk Update Chief Editor, Dennis Cox highlights some of the key issues that are likely to be of interest.

Principle 1: Board's Overall Responsibilities

The Board has overall responsibility for the bank, including approving and overseeing Management's implementation of the bank's strategic objectives, governance framework and corporate culture.

The paper refers to a "duty of care" and a "duty of loyalty". These are defined as follows:

> **duty of care**
> *The duty of board members to decide and act on an informed and prudent basis with respect to the bank. Often interpreted as requiring board members to approach the affairs of the company the same way that a "prudent person" would approach his or her own affairs.*
>
> **duty of loyalty**
> *The duty of board members to act in good faith in the interest of the company. The duty of loyalty should prevent individual board members from acting in their own interest, or the interest of another individual or group, at the expense of the company and shareholders.*

This is significant since it is placing the duty on the Board members apparently individually. Consequently where Board members are representing a single shareholder, for example, it will be hard for them to show that they are meeting this duty of loyalty. The concerns are clear – officers are essentially custodians acting on behalf of all customers and exercising fiduciary responsibility. In practice this is likely to result in changes to some Board memberships with perhaps an increase in Board diversity resulting.

Among their other responsibilities, board members and senior management are expected to define conduct risk based on the context of the bank's business. The BIS note that cases of misconduct have been identified as stemming from:

- the mis-selling of financial products to retail and business clients;
- the violation of national and international rules (tax rules, anti-money laundering rules, anti-terrorism rules, economic sanctions, etc); and
- the manipulation of financial markets – for instance, the manipulation of Libor rates and foreign exchange rates.

It is clear from this that there is a greater expectation that the Board and senior management will be directly concerned with ensuring that the firm meet these obligations and this is likely to mean that in practice they receive greater information on actions being taken to ensure regulatory compliance.

The board should set the "tone at the top" and oversee management's role in fostering and maintaining a sound corporate and risk culture. Management should develop a written code of ethics or a code of conduct. Either code is intended to foster a culture of honesty and accountability to protect the interest of its customers and shareholders. This is clarified later in the paper as follows:

In order to promote a sound corporate culture, the board should reinforce the "tone at the top" by:

- setting and adhering to corporate values that create expectations that all business should be conducted in a legal and ethical manner, and overseeing the adherence to such values by senior management and other employees;
- 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 the bank operate within the established risk appetite and risk limits;
- confirming that appropriate steps have been or are being taken to communicate throughout the bank the corporate values, professional standards or codes of conduct it sets, together with supporting policies; and
- confirming that employees, including senior management, are aware that appropriate disciplinary or other actions will follow unacceptable behaviours and transgressions.

The paper specifically requires that they establish, along

with senior management and the CRO, the bank's risk appetite, taking into account the competitive and regulatory landscape and the bank's long-term interests, risk exposure and ability to manage risk effectively.

Also within this principle Boards are required to:

- oversee the bank's approach to compensation, including monitoring and reviewing executive compensation and assessing whether it is aligned with the bank's risk culture and risk appetite; and
- oversee the integrity, independence and effectiveness of the bank's policies and procedures for whistleblowing.

The role of the remuneration committee as a sub committee of the Board is therefore clarified. Remuneration is a Board responsibility conducted on its behalf by the remuneration committee.

In another article we consider some recent compliance cases where action has been taken against compliance officers. In the light if these key requirements we would expect action to be taken against officers of the bank prior to action being taken against compliance staff.

Still within Principle 1 there is a discussion of risk appetite. Again this is within another article in this Update. However the specific requirements are as follows:

The bank's Risk Appetite Statement (RAS) 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.

This is still in our opinion a little confused and fails to actually assist firms with the implementation challenges which clearly will occur. Later in this Update we explain what risk appetite really means leading to a more acceptable and appropriate solution.

Principle 1 is a complex principle in the way it includes so many different issues. Thankfully many of the subsequent Principles are more straightforward.

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.

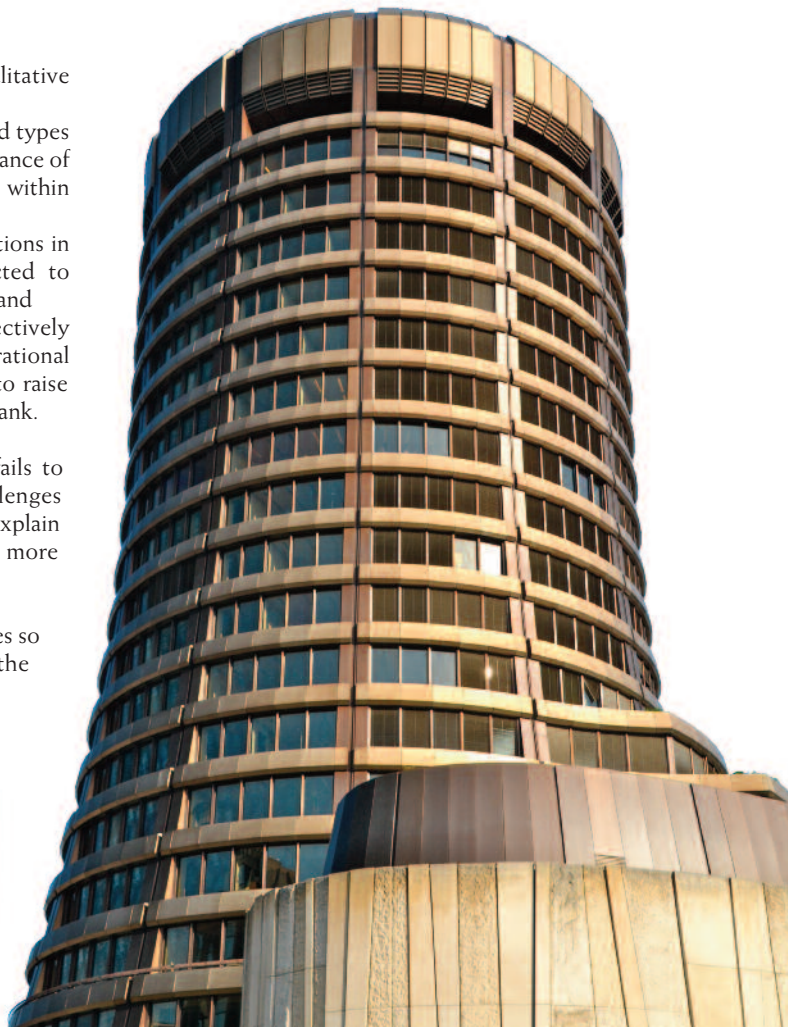
This has been carried forward from previous versions of the Principles. There needs to be sufficient independent directors who are free from bias. Individuals need a balance of skills, diversity and expertise with the Board collectively possessing necessary qualifications commensurate with the size, complexity and risk profile of the Bank. This is actually a little softer than the requirements being promulgated in Europe which required more of individuals.

The specific relevant areas of competence highlighted may include, but are not limited to capital markets, financial analysis, financial stability issues, financial reporting, information technology, strategic planning, risk management, compensation, regulation, corporate governance and management skills.

The remainder of the detail under this Principle essentially repeats previous papers.

Principle 3: 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.



Trying to Improve Corporate Governance

What is being requested is that Boards review whether their structure remains suitable for the business and regulatory environment. Too often structures have been developed over time without the necessary time being spent to ensure that they continue to be effective. Often we find that it is the failure of the corporate structure that leads to the problems faced in practice. The requirements are detailed and specific. They state the following:

To support its own performance, the board should carry out regular assessments – alone or with the assistance of external experts – of the board as a whole, its committees and individual board members. The board should:

- periodically review its structure, size and composition as well as committees' structures and coordination;
- assess the ongoing suitability of each board member periodically (at least annually), also taking into account his or her performance on the board.
- either separately or as part of these assessments, periodically review the effectiveness of its own governance practices and procedures, determine where improvements may be needed, and make any necessary changes; and
- use the results of these assessments as part of the ongoing improvement efforts of the board and, where required by the supervisor, share results with the supervisor.

The suitability assessments are particularly relevant for the independent non executive directors to ensure that they remain independent and effective. Generally we would expect an independent firm to be appointed to conduct this work and our firm has fulfilled this role multiple times.

There is then the following interesting statement. "The board should maintain appropriate records (eg meeting minutes or summaries of matters reviewed, recommendations made, decisions taken and dissenting opinions) of its deliberations and decisions. These should be made available to the supervisor when required."

Too often dissenting statements are not minuted. It is clear from this that the expectation is that such statements will in future be minuted.

The requirements of the Audit Committee which appear in BCBS 280 also appear here as follows:

The Principle states that the audit committee is, in particular, responsible for:

- framing policy on internal audit and financial reporting, among other things;
- overseeing the financial reporting process;
- providing oversight of and interacting with the bank's internal and external auditors;
- approving, or recommending to the board or shareholders for their approval, the appointment, remuneration and dismissal of external auditors;
- reviewing and approving the audit scope and frequency;
- receiving key audit reports and ensuring that senior management is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with policies, laws and regulations, and other problems identified by auditors and other control functions;
- overseeing the establishment of accounting policies and practices by the bank; and
- reviewing the third-party opinions on the design and effectiveness of the overall risk governance framework and internal control system.

The Risk Committee is also discussed and it now appears as a key required committee. In terms of their role the risk committee should:

- be required for systemically important banks and is strongly recommended for other banks based on a bank's size, risk profile or complexity;
- be distinct from the audit committee, but may have other related tasks, such as finance;
- have a chair who is an independent director and not the chair of the board or of any other committee;
- include a majority of members who are independent;
- include members who have experience in risk management issues and practices;
- 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;
- be required to review the bank's risk policies at least annually; and
- oversee that management has in place processes to promote the bank's adherence to the approved risk policies.

This is quite a change with the requirements for independent directors to be the majority being a major shift. Where these are all coming from may be a difficult question to answer!

Other specialised committees that are recommended include:

- **Nomination / human resources / governance committee:** provides recommendations to the board for new board members and members of senior management. The nomination committee should analyse the role and responsibilities of the board member and the knowledge, experience and competence which the role requires. Where a supervisory board or board of directors is formally separate from a management board, objectivity and independence still need to be ensured by appropriate selection of board members. The nomination committee should strive to ensure that the board is not dominated by any one individual or small group of individuals in a manner that is detrimental to the interests of the bank as a whole. It may be involved in assessment of board and senior management effectiveness and may be involved in overseeing the bank's personnel or human resource policies (see Principle 2).
- **Ethics and compliance committee:** ensures that the bank has the appropriate means for promoting proper

decision-making, due consideration of the risks to the bank's reputation, and compliance with laws, regulations and internal rules.

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, remuneration and other policies approved by the board.

Much of the detail here repeats previous standards. There is however a slight enhancement in reporting expectations as follows:

Senior management should provide the board with the information it needs to carry out its responsibilities, supervise senior management and assess the quality of senior management's performance. In this regard, senior management should keep the board regularly and adequately informed of material matters, including:

- changes in business strategy, risk strategy/risk appetite;
- the bank's performance and financial condition;
- breaches of risk limits or compliance rules;
- internal control failures;
- legal or regulatory concerns; and
- issues raised as a result of the bank's whistleblowing procedures.

Notice that the obligation is on the Board rather than committees of the Board so this could result in additional reporting of detail to the Board. I would recommend that the greater detail be available and key messages be summarised for the Board to consider. Again reporting needs to be consistent with risk appetite expectations to prevent time being wasted on immaterial matters.

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 the establishment and operation of 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 group's organisational structure and the risks that it poses.

The detailed analysis of this principle focuses on parent and subsidiary boards together with opaque structures. There is little that is new here however they do clarify responsibilities of senior management and the board, as appropriate noting that they should be cognisant of the challenges and take action to avoid or mitigate them by:

- avoiding setting up complicated structures that lack economic substance or business purpose;
- continually maintaining and reviewing appropriate policies, procedures and processes governing the approval and maintenance of those structures or activities, including fully vetting the purpose, the associated risks and the bank's ability to manage those risks prior to setting up new structures and initiating associated activities;
- having a centralised process for approving the creation of new legal entities and subsidiaries based on established criteria, including the ability to monitor and fulfil each entity's regulatory, tax, financial reporting, governance and other requirements and for the dissolution of dormant subsidiaries;
- establishing adequate procedures and processes to identify and manage all material risks arising from these structures, including lack of management transparency, operational risks introduced by interconnected and complex funding structures, intragroup exposures, trapped collateral and counterparty risk. The bank should only approve structures if the material risks can be properly identified, assessed and managed; and
- ensuring that the activities and structure are subject to regular internal and external audit reviews.

Principle 6: Risk management function

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.

The paper notes that the Key activities of the risk management function should include:

- identifying material individual, aggregate and emerging risks;
- assessing these risks and measuring the bank's exposure to them;
- subject to the review and approval of the board, developing and implementing the enterprise-wide risk governance framework, which includes the bank's risk culture, risk appetite and risk limits;
- ongoing monitoring of the risk-taking activities and risk exposures in line with the board-approved risk appetite, risk limits and corresponding capital or liquidity needs (ie capital planning);
- establishing an early warning or trigger system for breaches of the bank's risk appetite or limits;
- influencing and, when necessary, challenging decisions that give rise to material risk; and
- reporting to senior management and the board or risk committee on all these items, including but not limited to proposing appropriate risk-mitigating actions.

The issue of independence is discussed. Recently we have seen a number of risk functions which have been embedded within business units. This is clearly not an ideal situation and the BIS state that while it is common for risk managers to work closely with individual business units, the risk management function should be sufficiently independent of the business units and should not be involved in revenue generation. Such independence is an essential component of an effective risk management function, as is having access to all business lines that have the potential to generate material risk to the bank as well as to relevant risk-bearing subsidiaries and affiliates.

Trying to Improve Corporate Governance

The paper goes on to discuss the role of the Chief Risk Officer (CRO) although this repeats material previously issued.

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.

At this point it is probably worth reminding you that this is a corporate governance paper and not a risk management paper. There are a lot of sound practices papers governing risk management already in issue and this paper does to some extent reiterate key elements. That so much of this paper addresses risk highlights the importance of this issue to Boards and their memberships.

Because it was the operational risk sound practices paper which introduced many key risk building blocks too often risk functions delegated risk identification to the operational risk function. This paper makes it clear that risk identification needs to cover all risks. The importance of stress testing is again emphasised although there is a separate sound practices paper on this specific issue. This paper emphasises the role of the Board as follows:

As part of its quantitative and qualitative analysis, the bank should utilise stress tests and scenario analyses to better understand potential risk exposures under a variety of adverse circumstances:

- internal stress tests should cover a range of scenarios based on reasonable assumptions regarding dependencies and correlations. Senior management should define and approve and, as applicable, the board should review and provide effective challenge to the scenarios that are used in the bank's risk analyses;
- reverse stress testing could provide additional insight into the risk position of the bank as well as potential future management actions;
- stress test programme results should be periodically reviewed with the board or its risk committee. Test results should be incorporated into the reviews of the risk appetite, the capital adequacy assessment process, the capital and liquidity planning processes, and budgets. They should also be linked to recovery and resolution planning. The risk management function should suggest if and what action is required based on results; and
- the results of stress tests and scenario analyses should also be communicated to, and given appropriate consideration by, relevant business lines and individuals within the bank.

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.

Requesting dynamic forward looking reporting there is little that is new here.

Trying to Improve Corporate Governance

Principle 9: Compliance

The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should establish a compliance function and approve the bank's policies and processes for identifying, assessing, monitoring and reporting and advising on compliance risk.

Of course compliance risk within the BIS framework is an element of operational risk albeit that reputational risk is a separate risk category. The paper requires that the compliance function be independent from management to avoid undue influence or obstacles as that function performs its duties. It states that the compliance function should directly report to the board, as appropriate, on how the bank is managing its compliance risk. Again as mentioned later in this paper it can be senior management that directs compliance to do the wrong thing and then of course a whistleblowing charter is required even though the compliance officer may never work again.

Principle 10: Internal audit

The internal audit function should provide independent assurance to the board and should support board and senior management in promoting an effective governance process and the long-term soundness of the bank.

Again there is a separate sound practices paper on internal audit in banks so was this really required? By including it here at least the BIS are emphasising its importance.

There is nothing here that had not already been issued by the BIS.

Principle 11: Compensation

The bank's remuneration structure should support sound corporate governance and risk management.

This reiterates what appears in Principle 1 and other papers. It specifically states that remuneration should reflect risk-taking and risk outcomes. Practices by which remuneration is paid for potential future revenues whose timing and likelihood remain uncertain should be carefully evaluated by means of both qualitative and quantitative key indicators. The remuneration framework should provide for variable remuneration to be adjusted to take into account the full range of risks, including breaches of risk appetite limits, internal procedures or legal requirements.

Principle 12: Disclosure and transparency

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

Much of this repeats what appeared earlier in the paper and none of this is new.

Now for the supervisors:

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.

And that is it. There is a change of emphasis in some areas and a restatement of various obvious matters but it is perhaps in the review and organisation of the Board that the main changes exist together with the changing skills requirements. We expect Boards to require more risk based professionals as independent members and are already supplying such individuals as required.

For further information please contact:

Dennis Cox – CEO
telephone: +44 (0)20 7638 5558
email: DWC@riskrewardlimited.com

Lisette Mermod – New York
telephone: 1-917-310-1334
email: LM@riskrewardlimited.com

Tony Subryan – Public Relations
telephone: +44 (0)20 7638 5558
email: TS@riskrewardlimited.com