Chapter 8: Management of non-financial risks[136]

The Main Issues

The risk appetite of central banks is quite low, in part because they see risk as a threat to what is arguably their most important asset – their reputation. The risk management practices at central banks are more advanced with respect to financial risks than to non-financial risks. The principal issues to be confronted in pursuing a more proactive approach to the management of non-financial risks, the main focus of this chapter, are as follows:

- Are there net benefits to integrating the management of financial risk with that of non-financial risk? How much does the dominance of policy objectives over financial objectives influence this choice?
- How centralised should central bank risk management be? What roles should be played by top management and the oversight board? Should the risk of getting policy wrong be handled by the relevant policy committee or by a separate risk management committee?
- Most broadly, can central banks go beyond mechanical aspects of risk reporting to develop a genuine risk management culture?

As reputation is vitally important to central banks, their risk appetites have traditionally been relatively low. Without a good understanding of the risks faced, risk aversion may lead to an excessive bias towards conservatism. But central banks are now benefiting from risk mitigation that arises from a more conscious assessment of the risks embedded in their operations and policies. Prompted by the need to be accountable to their stakeholders, and drawing on advances in risk management techniques, they have become more systematic in their risk management by adopting more structured approaches and enhancing the oversight of their risk management activities. For some central banks, particularly those that supervise commercial banks, adoption of a more formal framework has also been driven by a desire to match the progress that commercial banks are making in implementing risk frameworks for compliance with Basel II.

The “bottom line” of central banks relates to policy rather than commercial outcomes. Nonetheless, as with commercial banks, risk management at central banks is more advanced with respect to financial than to non-financial risks. Accordingly, this chapter focuses on the opportunities available to central banks to enhance, and thus gain more benefits from, their management of non-financial risks.

[136] This chapter was prepared mainly by Bruce White. It draws heavily on the unpublished report of a study group that reviewed the organisation of risk management and methods for managing non-financial risk at central banks.

1. A risk management framework

Like many financial organisations, central banks often distinguish between financial and non-financial risk (Figure 46) and apply dedicated risk management structures. But even with separate management structures for the two risk types, risk management itself exhibits two key characteristics at central banks that have formalised it:

- Risk management has been identified as a strategic priority and thus elevated and broadened to apply across the institution.
- The management of operational and reputational risk and, to some extent, policy risk is wrapped within a standardised framework encompassing both financial and non-financial risk.

Key elements in any risk management framework include the identification of types of events that could compromise the achievement of the central bank's objectives, assessing the appetite for risk, putting in place measures to mitigate the risks that are deemed unacceptable, monitoring and managing risks over time, establishing contingency plans for risk events that may occur and regularly reassessing the adequacy of the risk management framework. As will be seen below, such arrangements at central banks are more developed with regard to financial risks.

Figure 46

Risk categorisation model

Source: BIS (2007a).

Governance arrangements for risk management typically consist of three components: overall responsibility, day-to-day management and systems to achieve a consistent approach across the institution. The overall responsibility for risk management lies with the institution's most senior level of management. Day-to-day risk management resides with departments, units and individuals. Consistency of approach across departments and units is promoted by adopting a common methodology; often (but not always), it is also promoted by a coordinating risk management unit which, among other things, condenses detailed risk management information into actionable monitoring reports.

The following summary of risk management frameworks begins with those for financial risks, partly for completeness but also to provide a background for the consideration of ways to strengthen non-financial risk management.

1.1 Financial risk

Financial risk management arrangements for central banks are fairly similar to those in place in commercial banks. The main elements are:

- a risk management committee, comprising senior executives and typically chaired by a deputy governor, with overall responsibility for risk management frameworks and policies (as is the case at, for example, the Reserve Bank of Australia, the Central Bank of Chile, the Bank of France and the Bank of England);
- a framework of delegated authorities and risk limits (credit, duration and position limits);
- a separation of duties between front and back offices to facilitate effective control arrangements;
- a risk management unit (or "middle" office) that monitors risk against limits and is responsible for risk analysis and support. This unit may be co-located with the portfolio managers or be separate and independent of them. Internal control principles suggest the latter approach, although many central banks find that co-location is beneficial in terms of achieving appropriate integration of risk management into business operations (and vice versa). However, central banks that adopt this approach acknowledge a need to ensure effective audit oversight; and
- an internal audit function, which has an independent compliance role, with direct reporting lines to the governor, or the supervisory board, or both.

The middle offices, using dedicated tools and techniques and staff trained in financial modelling, are common in central banks that take active financial risks. Likewise, specialised operational risk officers are commonly located in divisions that give rise to operational and business continuity risks. Areas in which the potential for fraudulent activity is elevated employ reconciliation and checking procedures that are stronger than those used elsewhere in the bank. And systems for reporting process failures tend to be more highly developed in areas in which weaknesses in business controls would cause the greatest problems.

1.2 Operational risk

As illustrated in Figure 46, operational risk encompasses a number of elements, including risks in relation to staff, IT systems, legal, regulatory and political risk, as well as human failure.

Transactional processes (eg operations for monetary policy, foreign exchange reserves, and banknote printing and delivery) involve risk of error or fraud; support activities (eg IT, human resource management, and physical security) may also cause financial, operational or image damages. Hence both transactional and support activities need to be subject to internal control procedures.

Management activities, such as decision-making and project management, are also prone to operational risk. But management activities are more difficult and even awkward to treat within an operational risk framework, given that decision-making under uncertainty, with incomplete information, is what management is about. But the risks can be mitigated through the adoption of robust project management and decision-making processes.

Economic analysis and research *processes* are also more difficult to integrate into an operational risk management process. Economic analysis inherently works in the

context of uncertainty; the definition of an operational failure is difficult, and the assessment of the consequences is not easy, even at the qualitative level. That does not mean, however, that the management of the risks cannot be improved. Obviously, risks linked to the availability and accuracy of data, the competencies of people, the efficiency of IT systems and the quality of internal procedures to meet qualitative and quantitative targets can be identified and managed.

1.3 Policy Risk

Many central banks regard the evaluation of economic risks and uncertainty as part of the interest rate decision-making process (or its equivalent in other areas of policy) and thus as a matter for the monetary policy committee rather than the risk management committee. Nonetheless, some central banks integrate policy risk management and overall risk management. For example, at the Bank of Canada, managers seek to identify and assess the key risks that could impede the fulfilment of the Bank's responsibilities and the achievement of its objectives. The results of the self-assessment process are summarised in a report to the Bank's management and discussed with the Board.

In another example, the HKMA had to consider risks to its reputation arising from consumer complaints about banking services, even though the matters in question went beyond the scope of the HKMA's supervisory function. The HKMA's Risk Committee examined the matter with a view to identifying options and avenues for addressing the risks, including the possibility of the need for change or refinement of policies.

In contrast, the risk management framework used by the Reserve Bank of Australia does not apply to the risks inherent in the Bank's core policy functions, which remain the responsibility of the respective policy boards. However, a failure to comply with, for example, procedures for implementing financial market transactions (for policy implementation purposes or management of foreign reserves) would be reflected in an *operational* risk event.

1.4 Reputational risk

Overarching the categories of financial, operational and policy risk is reputational risk. Reputational risk can be viewed as secondary, in that reputational damage usually is caused by a loss or failure in the areas of policy, operations or finance. But given the importance of credibility to central banks, reputational damage can be their greatest concern. In a 2003 BIS survey (BIS (2003b)), the vast majority of respondents reflected the view that continued reliance on the central bank as an independent authority with the necessary financial resources ultimately depends on trust in the institution.

Reputational risks can occur when there is a mismatch between public perceptions and the actual objectives and resources of the central bank. Serious misconduct, human or system failures or major difficulties in meeting objectives are not frequent among central banks, but they can seriously damage credibility when they do occur. Questions concerning ethical conduct and core principles such as honesty and integrity can pose a more severe test than purely legal issues, such as litigation against the organisation.

8

2. Organisation of risk management: the centralisation/decentralisation choice

Until relatively recently, central banks rarely integrated all risk management efforts in a single senior level body. Instead, a risk management committee at the senior management level would often focus on financial risks associated with active risk-taking in financial operations; the relevant policy committees would consider policy

related risks; and the senior executive board or committee would consider operational and general reputational risks. The degree to which senior management considered all risks in an integrated way would depend on the degree of common membership of these committees; and a comprehensive discussion of all risk issues would not be a regular agenda item for the bank's entire senior management.

Today, central banks are increasingly placing their various risk monitoring groups within an overall risk management framework that seeks to ensure consistency across the bank.

Many central banks have a risk management committee of several senior level officers that is chaired by the governor or deputy governor:

- The Reserve Bank of Australia and the HKMA both have risk management committees chaired by top management (the Deputy Governor at the Reserve Bank of Australia, the Chief Executive at the HKMA). Each committee reports to its institution's executive committee, and each is supported by specialised risk units.
- At the Bank of France, the risk committee dealing with financial risks is chaired by a deputy governor, and once a year the Executive Committee (chaired by the Governor) dedicates a meeting to operational risks.
- At the Bank of Spain, the Deputy Governor chairs the Operational Risk Management Committee, which reports to the Executive Commission.
- At the Swiss National Bank, financial and operational risk management share the same high-level governance structure. The Governing Board decides upon all strategic aspects of risk management, whereas the Risk Committee of the Board of Directors supervises the adequacy of the risk management processes and principles as well as adherence to them.
- At the Bank of England, governance oversight of the risk agenda is the responsibility of the Court, with some aspects delegated to its Audit Sub-Committee. An Executive level Business Risk Committee reports to the Court and recommends the overall parameters for risk appetite and policy – they are supported by a specialised Risk Oversight Unit. The Business Risk Committee's main objectives are to devise a risk management policy for the central bank, to determine the spectrum of risks that will be brought within the risk management framework and to ensure that they are assessed and managed by staff in accordance with these policies, particularly those risks that span more than one part of the central bank.

The accountability of senior management is enhanced by clear and regular reporting lines to the relevant oversight body on risk management – eg the board of directors or a parliamentary committee. The connection enables the oversight body to, when appropriate, endorse the risk management policy, to be apprised of the most significant risks facing the central bank, and to seek reasonable assurance that staff are trying to achieve the organisational objectives with an acceptable degree of residual risk. The appropriateness of the oversight body's involvement depends in large part on the ability to design procedures that avoid clashes with the central bank's autonomy on policy matters.

While risk management is generally viewed as a responsibility of senior management, practitioners also stress the crucial need for risk "ownership" to remain with the (generally lower) organisational units where individual risks actually arise. For example, at the Swiss National Bank, financial risk management is centralised but operational risk management is decentralised and parallels business line responsibilities. The Bank

of Mexico established a centralised department for financial risk management and created a coordinating risk management unit that reports to decision-making bodies primarily on operational risk issues. However, the responsibility for operational risk management resides within each department. That pattern shows that a consistent framework for the evaluation and reporting of risk issues can still allow for a high degree of specialisation at the operational level.

The optimal location of the middle office (risk analysis) function of the central bank's financial activities is an issue that is part of the broader centralisation/decentralisation topic. Most researchers and regulators agree that the front, back and middle offices of the financial markets area should be clearly separated; and these observers hold that the easiest way to achieve the separation is to make the middle office part of an independent risk management group with no organisational links to the financial markets area. However, several factors make many central banks reluctant to shift their middle offices from the markets area. They argue that, first, potential conflicts of interests are less significant in central banks simply because they do not pay profit-related bonuses. Second, they point out that middle office staff will maintain a much stronger familiarity with financial markets, instruments, trading processes and financial modelling by remaining part of the financial markets area. Last, central banks that have decided to maintain a middle office in the markets area point out that they have generally looked to strengthen governance and surveillance arrangements by, for example, upgrading audit oversight.

The Reserve Bank of Australia has recently taken the contrary approach, moving the middle office function from the Financial Markets Group to the Risk Management Unit. The purpose of the relocation was to have the front and middle office reporting lines come together in the Risk Management Committee.

3. Approaches and techniques for managing non-financial risks

The main elements of most risk management methods are:

- a risk taxonomy;
- a risk matrix; and
- a set of methodological steps.

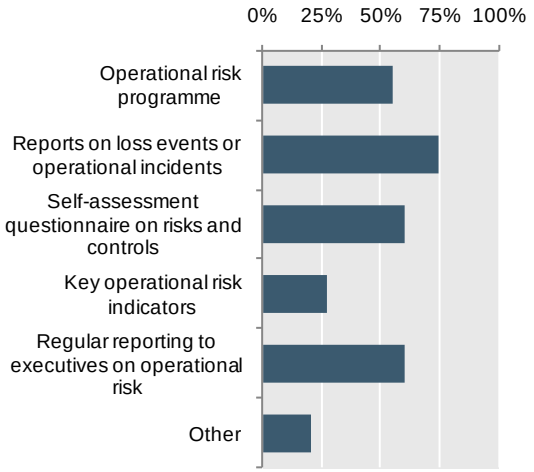
Together these provide a common language and methodology that employs both top down and bottom up approaches. Relevant tools include self assessment techniques, key indicators that show trends in risk "temperature", corporate risk scorecards, and databases of loss events. Several central banks have set up a business continuity committee to assure that business continuity plans are robust, coordinated, appropriately tested and updated to reflect changing threats.

A substantial number of central banks, particularly those with major supervisory responsibilities, tend to apply the Basel II framework for operational risk or the Enterprise Risk Management Framework devised by the Committee of Sponsoring Organizations (a private sector group aimed at reducing fraudulent financial reporting).

Figure 47

Operational risk tools and processes at central banks

Per cent of 40 central banks



Source: BIS (2008b).

Survey evidence suggests that a slight majority of central banks have a programme for managing operational risk.[137] The components of such programmes vary, but in most cases they include self-assessments and reporting (Figure 47).

3.1 Qualitative approaches: self-assessment

Most central banks with formalised approaches to risk management conduct some sort of regular (usually annual) self-assessment using qualitative risk rankings. For example, an operational component with a "high" risk rating would still be acceptable if the appetite for that particular risk was also rated "high" or above. Notably, the risk appetite of central banks tends to be higher for risks with limited scope for mitigation, and those risks are usually associated with the central banks' policy-driven actions.

Asking managers and staff to identify and assess risks helps increase awareness and responsibility and thereby improves the organisation's risk culture. The following techniques have been used by central banks in undertaking qualitative self-assessments:

- interviews;
- checklists and questionnaires;
- balanced scorecards - these are more elaborate checklists combining (with varying degrees of sophistication) the internal control assessment with the risk level of the domain; and
- workshops for business areas.

3.2 Quantitative approaches

A quantitative approach to risk management is to use data from event logs to model operational risk. The model in turn can yield measures – so-called key risk indicators – that point to emerging problems or losses.

3.2.1 Event logs

Reporting of loss events is an important component of the risk management programmes of a number of central banks. For a logging system to be effective, the staff must understand that the notation of loss events and incidents is a valuable action and not a trigger for blame. The challenge is to make it clear that a zero incident situation, like a zero risk situation, is either not possible or is achieved only at the cost of excessive control.

[137] Updated survey evidence and BIS (2007a).

At present, only a few central banks, for example, the Bank of Spain, capture explicit loss event data. These banks use a variety of approaches to gather the data, including using existing databases such as the general ledger or delegating collection responsibilities to a low level within the business unit, in most cases the operational risk liaison.

3.2.2 Key risk indicators

Key risk indicators are designed to measure the risk of major negative events. Only a handful of central banking institutions, for example, the Bank of England and the Federal Reserve's New York Reserve Bank, have thus far sought to develop key risk indicators as part of a formal risk management programme; and as with the commercial banks (which have been developing such indicators in the context of Basel II implementation), their work is at an early stage of development. That said, many central banks have informal processes to record and monitor certain key indicators, such as staff movements, staff training, operational health and safety incidents, and computer virus and other IT statistics.

3.3 Reputational risk management

The main method for dealing with the risk of damage to reputations is to manage the primary risks that would give rise to such an outcome. In addition, in relation to ethical standards and compliance issues, specific risk management tools are available. Post-event management can also affect the extent of reputational damage.

3.3.1 Public expectations

The central bank's high prestige can generate public expectations that go well beyond the legal responsibilities of the institution. And its position of power can generate doubts about integrity that are difficult to assuage. Thus, for example, in the case of exaggerated expectations, the central bank's reputation can suffer when individuals lose money in disputes with financial institutions, regardless of what the central bank's actual role in the matter may be. To the extent that the reputational damage spills over onto the central bank's effectiveness in relation to matters for which it does have both capability and responsibility, real harm can arise.

Regarding entrenched doubt, if the legal mandates of the central bank give rise to a potential conflict of interest, its reputation may also be at risk. An example is the central bank's compilation of macroeconomic statistics, which exposes it to the accusation that it is manipulating the data in its own interest. If the public cannot be satisfied that it can rely on the central bank's internal controls, resolution of the problem can involve a difficult choice: the responsibilities can be kept at the central bank to benefit from its autonomy and professional expertise (which, however, have come under attack in the charge of statistical self-dealing) or at a national statistical agency, where the integrity of governance arrangements and the level of expertise may not be beyond doubt. The problem has arisen in Mexico, where, in a third option, the task of computing price indices is in the process of being transferred to an autonomous statistical institute.

3.3.2 Factors beyond the central bank's control

The policy decision to hold net foreign exchange reserves, and thus a long foreign exchange exposure, can pose a risk to the central bank's reputation. When changes in the local currency value of these reserves create losses, the media and the public may blame them on weak management at the central bank. One way to address such risks has been adopted by the HKMA, ie maintain regular communication with the media and discussions in public, including legislators. Central banks can also seek arrangements under which the valuation gains and losses are shared with, or passed to, the government treasury.

3.3.3 Personal misconduct

As noted above, questions concerning ethical conduct can pose a more severe test to a central bank's reputation than purely legal issues, such as litigation against the organisation. To illustrate this, in 2003 a secretary to the Governor of the Central Bank of Chile was discovered to be leaking confidential information to a local financial firm from the Governor's office. The episode served to uncover a larger fraud operation in which other public entities were affected as well, and the information leaked by the secretary proved to be of little value. But the Bank's reputation was nonetheless at stake. It took the Governor's resignation to resolve the crisis, along with establishing very clearly that neither the Governor nor other central bank officials had been involved in the fraud. Even so, the Bank's reputation was damaged, and the episode revealed several flaws in its handling of the media.

Central banks manage the risks that can arise from personal misconduct generally through codes of conduct covering issues such as conflicts of interest, personal investments, acceptance of gifts received in the course of duty and political activity. In addition, some of these issues as they apply to the governor or board members are commonly incorporated into the central bank law.

3.3.4 Challenges in managing reputational risk

In managing reputational risk, central banks seek both to limit the causes that could initiate a reputational incident and to effectively manage an unfolding incident. Some of the steps central banks have taken in this regard include:

- Elevating staff awareness. The Bank of Canada requires business managers to assess the reputational implications of each business activity in the regular risk assessment.
- Evaluating initiatives before launch. The HKMA requires departments introducing major new services or policies to undertake a viability assessment to be monitored by internal audit. The Central Bank of Brazil is similarly strengthening strategic planning and project management to reduce reputational risk.
- Pre-emptively communicating. Public outreach in anticipation of problems can be an effective tool to manage public expectations, for example, in relation to the performance of a central bank's portfolio of foreign exchange reserves.
- Using data on complaints or dissatisfaction. Maintaining and regularly analysing a log of complaints and other events with reputational implications can provide the early warning signs of serious problems, and the data can help guide efforts to mitigate the risks and improve performance. In addition, some central banks engage external consultants to conduct discreet public opinion surveys on a regular basis to track the public's awareness of their work, as well as the public's satisfaction with and support for their policies and services.
- Implementing codes of conduct. A code of conduct reflects the core values of an organisation and the expectations of stakeholders and the community at large. But simply having the code does not suffice – regular staff training and occasional updating of the code are also needed.

4. Links to other central bank management issues

4.1 Internal audit and compliance

Both the private and public sectors have moved towards clearly separating risk management from auditing. For commercial banks, the Basel Committee on Banking Supervision (BCBS) has been a strong advocate of separating the functions and has recommended that the "internal audit function should not be directly responsible for operational risk management" (BCBS (2003)). The main motivation for the separation is to avoid the potential conflict of interest that can arise. In essence, if risk management is a management task and therefore subject to audit scrutiny, the audit area should not have an explicit role in the risk management process. That said, most risk management practitioners still advocate a close working relationship between the separated functions, in part to maintain consistency between the risk management and audit frameworks.

Differences in approach are evident across central banks. At the Bank of Mexico and the Bank of Spain, the Internal Audit Department is set apart from the central risk management function. At the Bank of France, the Risk Management Central Unit and the Audit Department are placed in the same General Directorate (General Control), but the relations between them are structured in a formal way consistent with their respective roles. Moreover, the Risk Management Central Unit is clearly auditable.

A number of (mainly smaller) central banks also carry out the two activities together in a single area, primarily owing to resource constraints. Various methods are available to help mitigate the potential conflict of interest identified above. For example, at the Reserve Bank of New Zealand, the risk management function is evaluated on a regular basis by external, rather than internal, auditors.

4.2 Change and the management of change

Central banks often have a system in place to ensure adequate levels of control over project design, approval and delivery. The system is likely to include some kind of assessment process for the risks related to project delivery. Although some of a project's benefits may be linked to the reduction of risk exposure within the business, it is important to keep the two views of risk separate – the former (the assessment process) is about risks to the project, the latter (benefits) about the risk profile in the business-as-usual state.

4.3 Business continuity and crisis management

Business continuity risks refer to the disruption of the bank's normal business operations as a result of a natural or man-made emergency such as fire, flood or terrorism. The risks can take many forms, but typically they are categorised into five generic events:

- loss of critical services;
- loss or severe degradation of communication or telephone networks, including mobile networks;
- acute failure of information systems or loss of data;
- absence of significant numbers of staff in one or more critical functions (eg flu pandemic, civil emergency); and
- loss of access to bank premises.

Business continuity planning (BCP) has become a critical component of operational risk management in the financial sector. In recent years, financial institutions, central banks and regulators have devoted significant resources to strengthening BCP to enhance the resilience of their national financial systems and to minimise the impact of a sudden failure of critical infrastructure as a result of terrorism or natural disasters. Some central banks, including the Reserve Bank of Australia, have established self-contained business resumption facilities to provide back-up capacity and business continuity in the event that access to head office facilities or IT systems is lost.

In some central banks, business continuity planning is conducted in the same area as the operational risk management function because such planning can mitigate the risk in some types of operational risk. A number of central banks have a central business continuity function that is part of the central risk team and forms a key part of the risk framework. This business continuity function sets the organisation's policy and standards for the format and content of local business continuity plans. An annual threat assessment reviews the priorities for business continuity plans and their updating. It is usual to have a business continuity committee that meets regularly to assure that the plans are robust, coordinated and appropriately tested and that they reflect changing threats.