MANAGEMENT ACCOUNTING – RISK AND CONTROL STRATEGY

The examiner for paper P3 examines the crisis at Northern Rock and considers whether it was caused by a failure of risk management.

PHOTOGRAPH: ALAMY

Perhaps the most interesting case study of risk and control strategy last year was that of Northern Rock. In September 2007 the bank was one of the top five UK mortgage lenders and was listed on the FTSE 100 with assets worth more than £100bn. The company had raised over 70 per cent of the money for its growing mortgage-lending business from banks and other financial institutions. When the global credit crunch resulted from a crisis in the US sub-prime mortgage sector, Northern Rock could no longer raise the cash to cover its liabilities.

A run on the bank by its customers prompted the government to provide "lender of last resort" funding and guarantees for depositors totalling about £20bn. The result was a 90 per cent decrease in Northern Rock's share price, a deteriorating credit rating and a loss of reputation. The chief executive resigned and several directors also left the board. The most likely scenario as *FM* goes to press is that Northern Rock will be taken over by another financial institution.

Northern Rock had a formal approach to risk management – covering liquidity, credit, operational and market risk – that it described fully in its filings for the US Securities and Exchange Commission (SEC). Its assets were sound, so there was no significant credit risk. Market risk was also well managed in terms of its exposure to fluctuations in interest and forex rates.

But, despite all its formal procedures and clear regulatory compliance, Northern Rock's managers had assumed that the bank's access to funds would continue unimpeded. The US sub-prime crisis caused a liquidity risk, which started Northern Rock's problems. Press reports then blamed its management for not having a contingency plan to cover disruption to its funding – an operational risk.

This case perhaps best illustrates the importance of balancing conformance with performance, as promoted by *Enterprise Governance – Getting the Balance Right*, a joint report in 2004 by the International Federation of Accountants (IFAC) and CIMA (http://snipurl.com/1wdhv). Conformance takes place through assurance, ensuring that the organisation understands and manages its risks effectively. The performance aspect identifies the need to take risks to achieve objectives. In order to do this, risk management has to be integrated with decision-making at every level. Northern Rock's SEC filings give the impression that its main concern was regulatory conformance, rather than its overall control environment.

CIMA members and students need to be constantly aware of the need to identify, evaluate, mitigate and monitor risks in their organisations. Business strategy, financial strategy, and risk and control strategy (not limited to financial risk) are distinguishing features of the syllabus, as identified in the institute's recent report, *The CIMA Difference* (http://snipurl.com/1wdad). This publication concluded: "CIMA people go way beyond accountancy – they use their skills to provide analysis, decision support, value creation and risk management."

IFAC's publication in 2006 of its *Internal Controls – A Review of Current Developments* report (http://snipurl.com/1wfvk) serves as a timely reminder to P3 candidates of the importance of knowing the current state of play in governance, risk and control as they prepare for their exams. A key role for a board of directors is to understand the significant risks an organisation faces and ensure that appropriate controls are in place. The IFAC paper stresses that the risk-based approach to internal control encompasses every one of an organisation's activities. The approach takes a much wider view than those relating to financial reporting – the emphasis of the Sarbanes-Oxley Act 2002 (Sox), which applies to all companies listed in the US, and typified by Northern Rock. Under this approach, internal control is fundamental and risks are defined broadly, covering not only what might go wrong but also the risk of a failure to achieve organisational objectives.

This broader view has been emphasised in the US by the Committee of Sponsoring Organizations of the Treadway Commission (Coso) in its *Internal Control – Integrated Framework* (1992) and *Enterprise Risk Management – Integrated Framework* (2004). It's also been endorsed in the UK by the Turnbull report, which is now part of *The*

Combined Code on Corporate Governance issued by the Financial Reporting Council (FRC). Coso has influenced the approach taken in relation to IT governance in *The Control Objectives for Information and Related Technology*, the latest version of which was published in 2005. The Coso/Turnbull model has been adopted in Canada, in Hong Kong by the stock exchange and in Europe by the Fédération des Experts Comptables Européens. Similar approaches have also been used in South Africa under the King report (known as King II) and, despite its two-tier board system, in the Netherlands. Australia largely follows the UK model in its company law economic reform programme (Clerp 9). All of these countries rejected a Sox-style regime.

The principles-based Coso/Turnbull method, where risk management and internal control is embedded in organisational processes, contrasts with Sox's narrower, rules-based framework. Under Sox, annual reports must include a statement that the management team is responsible for establishing and maintaining adequate internal controls for financial reporting, plus an assessment of the effectiveness of those controls. This assessment has to be reported on by the auditors. These requirements have reportedly increased both management compliance costs and audit costs in US-listed companies. In contrast, the UK does not require auditors to express a view publicly on the effectiveness of a firm's internal controls. IFAC's 2006 report recognised that Sox's focus on internal control for financial reporting could lead boards to see internal control as a compliance issue rather than part of managing a successful business – Northern Rock's filings complied with Sox, but this didn't save the bank from significant problems.

In September 2007 Coso produced a discussion document furthering its *Internal Control – Integrated Framework*. This paper (http://snipurl.com/1wg3a) provides guidance on monitoring internal control systems, arguing strongly that ineffective monitoring leads to a breakdown of control. This can happen if processes or risks change and controls do not adapt accordingly, or where previously effective controls cease to work as intended. In Northern Rock's case, risks changed in the credit crunch after the US sub-prime mortgage crisis, while previously effective controls in the bank's liquidity risk strategy failed because of the changes.

> "Northern Rock's filings complied with Sox, but did not save the bank from significant problems"

The Coso discussion document recommends that controls should be monitored via a structure that includes a change identification process, a change management process and the re-confirmation of control using various sources of evidence. It discusses different types of information that can be used in monitoring, depending on the importance of the controls and the underlying likelihood and significance of the risks.

Internal control is inextricably linked with corporate governance, since it's the board's role to monitor significant risks and the effectiveness of internal controls in managing those risks. It's likely that Northern Rock's board failed in monitoring both liquidity risk and the effectiveness of the existing controls.

CIMA members and students should, therefore, keep abreast of changes in corporate governance. First, in 2006 Coso published *Internal Control over Financial Reporting – Guidance for Smaller Public Companies* (http://snipurl.com/1wg4s), which provided 20 basic principles that would help to ensure compliance with the Sox requirements for internal control in financial reporting. The principles cover the control environment, risk assessment, control activities, information, communication and monitoring.

Second, in 2007 the FRC reviewed *The Combined Code on Corporate Governance* and, although it found the code was working well and needed no big changes, it did propose two amendments. The first proposal is to let an individual chair more than one FTSE firm and the second is to allow the chairman of a smaller listed company to be a member of the audit committee where he or she is considered independent on appointment. Any revisions to the code will not be made until this summer.

Lastly, a 2007 report for the Department for Business, Enterprise and Regulatory Reform by King's College, London, considered the key factors behind good corporate governance and how effectively the government's policies were promoting best practice. The document identified 18 key mechanisms for corporate governance, including board independence, shareholder activism, information disclosure and internal control. The researchers identified policy gaps mainly relating to executive remuneration, employees and stakeholders generally. They argued that it was important to balance and recognise trade-offs between mandatory regulations and "soft law" such as codes based on "comply or explain" principles, as well as the cost of regulation. This brings us back to the model proposed by CIMA and IFAC in *Enterprise Governance – Getting the Balance Right*.

The key lessons of the Northern Rock crisis are that companies need to move beyond ticking boxes, and that good corporate governance requires more insight into risk management and internal control. This is indeed *The CIMA Difference*.

Exam practice

Once you've read this article, try to answer the following question: discuss how Northern Rock might have applied a risk management approach to its liquidity risk.

Look for the model answer in CIMA's new student e-newsletter, the first issue of which will be e-mailed later this month.

P3 further reading

News updates on governance and internal control are available from the Financial Reporting Council at www.frc.org.uk/corporate.
The King's College report for the Department for Business, Enterprise and Regulatory Reform is available at http://snipurl.com/1wgfx.