Risk Reward
riskupdate
The quarterly independent risk review for banks and financial institutions worldwide
Q1 – 2010

New Standards for Risk Management

Also in this issue

MODERNISING THE INTERNAL AUDIT FUNCTION

Tariq Khan, B.Com, FCA, PIOR, is the newly appointed Head of Risk Based Internal Audit at Risk Reward Ltd. As head of internal audit at a leading international Japanese investment bank he set up a cutting edge risk based audit function and played a pivotal role in the establishing of the Audit Committee along Turnbull guidelines. In this first in a series of articles on the changing role and the impact of bank internal audit he describes the Basel Committee guidance to this changing and critical function within a regulated bank.

In 1998, when the Basel Committee issued its paper titled "Framework for Internal Control Systems in Banking Organisations" the role of the audit function was for the first time given formal recognition. Principle 11 states:

"There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the systems of internal control, should report directly to the board of directors, or its audit committee and to senior management."

It also emphasised, in principle 4 of the same paper, that internal control systems will be deemed ineffective if they do not consider and recognise material risks in their design. Thus, for the first time risk assessment was formally linked to sound systems of internal controls. Although some institutions were already practicing risk based auditing, it was not until this paper was issued that it got official recognition.

Recently, the Basel II Accord has reaffirmed these principles by stipulating that internal audit would have to capture in a larger way the application and effectiveness of risk management procedures and risk assessment methodology and critical evaluation of the adequacy and effectiveness of the internal control systems.

Basel II talks about risk based auditing in the context of management of operational and credit risk only, however, it has specific relevance to banks operating in emerging markets that are in the process of, or considering, implementing the accord. Whilst here in the UK we have had more than 10 years to practice risk based auditing, banks operating in emerging markets have now been forced to play catch up.

While the concept is straightforward, the application of a risk-based audit approach has taken many forms, from a once a year simple assessment of risk based on criteria defined by internal audit, or the board where these are available, to a much more complex model based approach where audit priorities and frequencies are reviewed and changed more frequently after considering the internal risk matrices of the bank. The choice depends upon the sophistication and risk maturity of the bank, capability of its audit team and the way in which the host regulators have translated these principles into their rule books.

Given the variety of risk-based forms available, for banks operating in the emerging markets, it is not a simple matter of just adopting a standard approach to risk-based audit as in practice there is no such thing. So what should a bank do when faced with modernising, or indeed establishing a new, audit function and what are the common traps that can endanger or derail its plans? It is perhaps best to discuss this question in the light of the UK experience. Why UK? Because perhaps the UK regulator has been the most advanced and successful regulator in the world in raising the profile and encouraging the firms under its supervision to take internal audit seriously.

Regulatory expectation

The interest in the audit function within the senior executive ranks has mostly been motivated by regulatory concern, which in itself is inextricably linked to external events such as a bank failure. In the UK, this interest began with the introduction of the new Banking Act of 1987. Section 39 (s39) of this Act gave the Bank of England (BoE), predecessor regulator to the Financial Services Authority (FSA), the powers to obtain an "Accountant's Report" on the whole or part of the operations of the bank. This power was used extensively by the BoE providing a bonanza for the "big 6" accountancy firms of the time. These Accountants' Reports tended to provide detailed analysis of the operations of the bank and in so doing uncovered many weaknesses in the control systems, which naturally led to recommendations for the establishment, or modernisation, of audit departments. It could be argued therefore that the credit for elevating the status of internal audit should really first go to the reporting accountants.

Since 1987 the role of internal audit has gradually gained more recognition in regulatory circles. But as mentioned above, it was the Basel paper in 1998 that propelled the audit function into the limelight. The successor supervisory body of the BoE, the FSA adopted these principles in its rulebook and under the heading of "Corporate Governance" set about transforming boardrooms and the audit function. Part of this emphasis on internal audit was related to costs. It was recognised, mostly from the experience of s39 reports, that supervision on the scale being envisaged would be very expensive. Their solution was allowing the banks, as long as they behaved, a kind of limited "self regulation" in which internal audit and compliance functions were at the forefront.

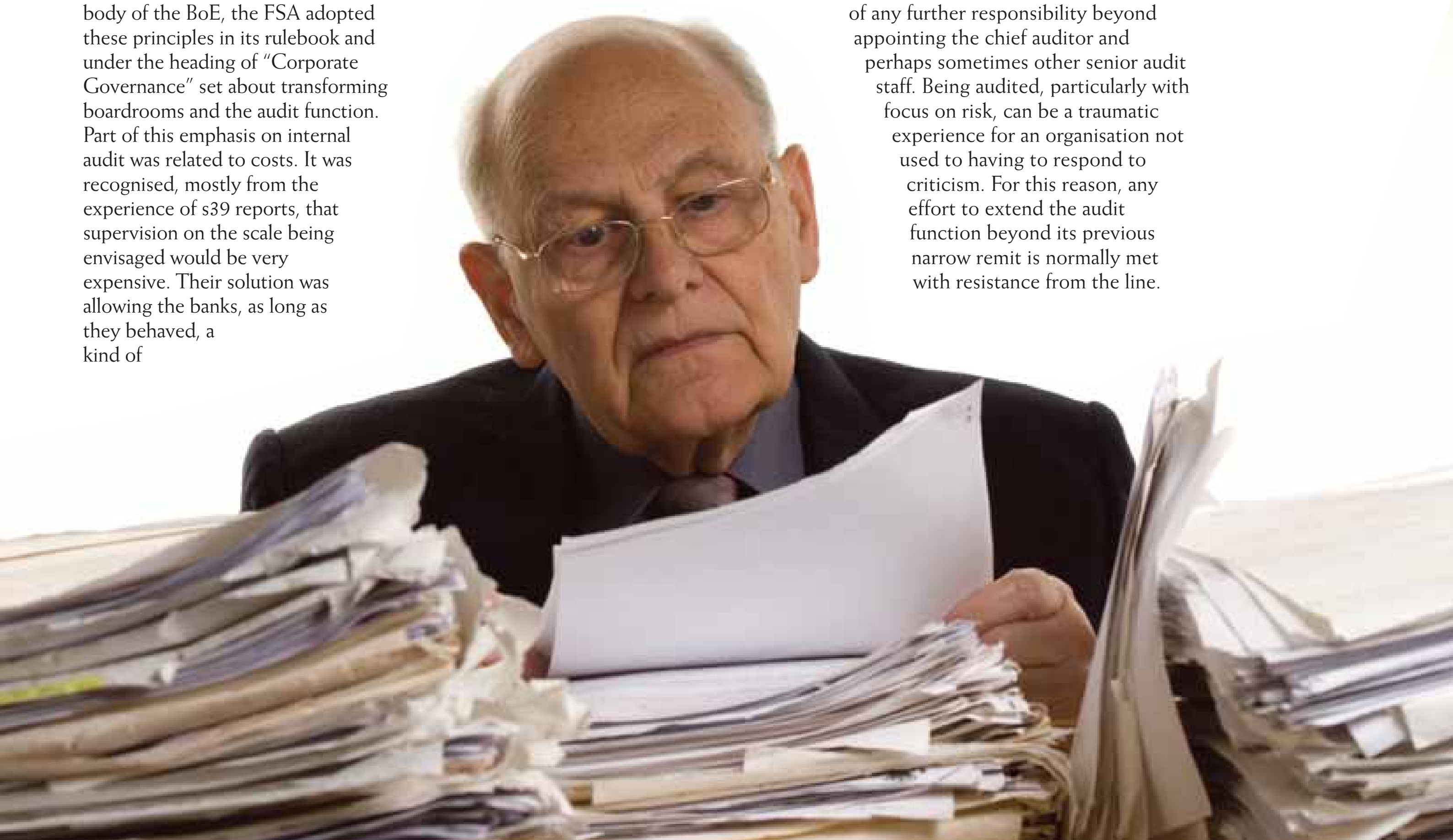
The FSA now expects to be able to rely on the internal audit function as a "third line of defence" and in exchange it promises reduced supervisory enquiries and visits, which anyone who has gone through one of these knows very well can soak up immense management time and resources. So it is clearly in the interests of the FSA regulated firms to demonstrate that they have a strong robust internal audit function. Conversely, failures in internal audit will invariably lead to questions about its corporate governance which would in turn affect the credibility of the bank as a whole. It could also prove costly if the FSA demands a s166 report which is the successor to the s39 report mentioned previously. As a last resort, the FSA is also quite prepared to slap additional capital charges where they find that management have not taken serious steps to enhance and support the audit function.

The establishment, or extent of modernisation, of an audit function in emerging markets will clearly depend upon the way in which the host regulators will translate, or already have translated, the Basel principles into its rulebook. This in turn also depends upon the ambitions of the authorities in each jurisdiction to modernise its financial industry and its eagerness to gain international recognition as a centre of finance. The regime for penalties and punishments in each regulatory jurisdiction will also be a powerful factor for a bank in its approach to corporate governance and internal audit.

Supporting the audit function

Without any shadow of doubt, the success of the audit function depends upon the support executive management are willing to give to it. As demonstrated above, in the UK, senior executives interest in the audit function has mostly been motivated by regulatory concern. It is very rare to find an enlightened bank executive that fully understands the value of internal audit and of his own volition is prepared to invest, nurture and support it. But without this support internal audit cannot function properly. Frustration will set in quickly and most good people will simply head for the door. High turnover in an audit department is always an indication that something is amiss and it won't be long before the regulator will start asking questions.

In the UK, the common mistake of management was to absolve themselves of any further responsibility beyond appointing the chief auditor and perhaps sometimes other senior audit staff. Being audited, particularly with focus on risk, can be a traumatic experience for an organisation not used to having to respond to criticism. For this reason, any effort to extend the audit function beyond its previous narrow remit is normally met with resistance from the line.



The involvement of the CEO in any modernisation programme is therefore a must if it is to succeed. Indeed, in the UK it is in his/her self-interest to ensure that it does. It is common to find that failings in corporate governance and internal audit have normally been blamed on senior management, especially the CEO, to whom the regulators invariably turn to for fixing the problems.

Support from the CEO, and his/her team, for the internal audit function has to be continuous and persistent. It is important to communicate regular statements of support for the audit function to senior and line managers. Meeting the head of audit and other members of the team on a regular basis to monitor their progress is important in ensuring that everyone in the organisation knows that the function is being fully supported at the top.

Audit Committees

The notion that internal audit should report to an audit committee is not new in the UK. Historically, the focus on Audit Committees came from the Combined Code on Corporate Governance, which has existed in various guises since 1992. Although many large commercial banks had functioning Audit Committees, their relationship with Internal Audit was superficial. It was not uncommon to find internal audit chiefs allocated only 15 minutes in audit committee meetings. In sharp contrast with their peers in other non-financial sectors, the banks executives did not pay much attention to the Combined Code until the new UK regulator, the FSA adopted the Basel paper in 1998.

Nowadays, it is widely recognised that no modernisation of internal audit can be complete without a properly functioning Audit Committee. Even foreign branches and subsidiaries operating within the UK tend to form some semblance of an audit committee.

In the UK, the FSA insist that not only an audit committee be formed but it must also comprise a majority of independent non-executive directors (NED's) and also that it be chaired by an independent NED, who should also meet with the chief auditor on a regular basis. The chair is also often required by the regulators to meet each senior auditor separately to gauge his or her competence and report back to the Committee.

Ideally the Chief Auditor should report directly to the Chair of the Audit Committee. According to the newly appointed Chair of an Audit Committee for a major bank in the UK: "how else can I assure myself of the independence of the audit function?" The same Chair also insisted on being the budget holder for the function and had full responsibility for staffing matters.

In practice, however, the chief auditor tends to have a reporting line to the CEO for pay and rations and other staffing matters and a dotted line to the chair of the audit committee for matters of governance. Both the CEO and the chief auditor have to tread a careful line though as the effectiveness of the Audit Committee and its relationship with the internal audit function can often be compromised.

Executive directors not used to working with Audit Committees can often exert undue influence by insisting that all communication between internal audit and the chair of the audit committee go through them first, thus effectively controlling the flow of information to the Committee. This can also adversely affect the relationship between the chief auditor and the Chair and also the chief auditor and the CEO. Because of the dependence of regulators on internal audit, they tend to talk to auditors during almost all of their visits and it is only a matter of time before they start examining this area.

One way of avoiding any undue influence from management on the relationship between internal audit and the audit committee is to state as a matter of policy that the chief auditor and the chair of the audit committee shall have unfettered access to each other at all times.

Appointment of senior audit personnel

Without doubt, the appointment of the chief auditor is a first and very significant step in the modernisation of the audit function. The chief auditor is the face of the internal audit function, he will make an immediate impression on how the whole function is perceived by others inside, and equally outside, the business. The chief executive needs to take a personal interest in the selection process. Whilst suitable qualifications and experience are always important, temperament and cultural fit are equally significant. You don't need to end up with someone who will upset everyone in the organisation but equally you also don't want someone who is unable to hold his own in a confrontation and failing to protect the wider interests of the bank.

Managing the inspection department

In many larger banks in the UK, audit had sort of existed in the form of Inspections for decades before. Contrary to being regarded as a backwater, positions in inspection departments were highly sought after. Branch managers, and their able assistants who themselves were being fast tracked to management positions, saw a stint in the inspection department as a necessary prerequisite into more senior roles at the head office. Inspectors also tended to be typically long serving members of the staff, with informal networks and close personal relationships around the bank.

Creation of a new audit department resourced by outsiders on probably higher salaries than inspectors, inevitably caused friction. This was also a time of industry restructuring and upheavals brought about by deregulation, which made an already fractious situation volatile especially as the line positions that the inspectors were looking to walk into suddenly started to disappear.

The UK experience shows that the capacity of long serving members of the function to disrupt the modernisation process and allow it to settle properly and embed in the organisation should not be underestimated. Little things can irk their wrath with disastrous consequences. For example, at one bank some inspectors successfully persuaded the executive responsible for audit and inspection to have the newly created audit function "inspected". It transpired later that their main motivation behind this manoeuvre was anything but altruistic. Apparently, the inspectors were the same grades as audit managers. They felt very strongly that if they cannot have offices of their own, neither should the managers in audit. This personal agenda eventually led to a wholesale reorganisation of the audit function. After that the relationship between the two functions never truly recovered. The resulting infighting eventually led to the replacement of the audit and inspection executive but by that time the damage had already been done.

Managing the disruptive elements of the inspection department, or an existing audit department, should be high on the agenda of the chief executive and should not be left to the head of the respective functions to sort it out between themselves.

Laying the boundaries

Modernising the internal audit function is likely to expand the scope of internal audit work into areas that until now have not been subjected to such an examination. To avoid confusion, it is important that there are clear boundaries within which internal audit is to operate. The setting of these boundaries is the responsibility of the board, or its audit committee, which it normally discharges by giving a mandate to the internal audit function, naturally in consultation with the chief auditor. In fact, good corporate governance necessitates that mandates are similarly awarded to risk, compliance and other governance functions as well.

To be effective the terms of reference should be clear and unambiguous. It is common these days, probably inspired by the new definition from the Institute of Internal Auditors (IIA), to see phrases such as assurance, consulting activity, add value, etc. creep into audit mandates. Phrases like these tend to obfuscate rather than provide a meaningful understanding in clear and unambiguous terms of what internal audit is all about and crucially what is expected of it[1].

However, it must be stressed that in internal audit matters, the regulators in the UK are influenced by the IIA and expect the internal audit function to at least provide some ad hoc consulting work which they often call consultancy or value added work. Besides undermining normal internal audit work by implying that it does not add value, these are also misleading terms. Typically many internal audit functions reserves 20-25% for special work such as for fraud or other incident investigations, new system development projects and other advice on internal control matters that inevitably get sought by line from time to time. All of this work is perfectly legitimate for internal audit to get involved with as long it does not compromise its objectivity and independence. The only difference here is that this work tends to be ad hoc one off assignments specifically requested by management as opposed to the majority of the recurring work that is determined by a risk assessment process.

Management should also be careful not to succumb to demands from their line managers to get internal audit to do work which essentially is the responsibility of the line. The most common requests tend to be for drafting of policies and procedures. Asking them to review already written policies and procedures is of course a reasonable request and should be considered under internal audit's special work.

Finally, it must be recognised that the modernisation process can take some years before it can be properly established and embedded into the organisation. During this time a lot of changes can occur in the regulatory, economic and business environment, which will involve re-evaluating the governance framework and the structure of the internal audit function. Keeping apace with new developments not only keeps the regulators sweet but also ensures that the best talent is attracted to the function.

---

[1] I prefer a more traditional definition such as "To provide an independent opinion by an objective assessment and evaluation of the systems of internal controls, designed, installed and operated by management, and to report to management on their adequacy and effectiveness".

For further information please contact:

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

Lisette Mermod – New York
telephone: 1-914-619-5410
email: LM@riskrewardlimited.com

Tariq Khan
telephone: +44 (0)20 7638 5558
email: TSK@riskrewardlimited.com