Risk Reward
riskupdate
The quarterly independent risk review for banks and financial institutions worldwide
JAN 2011

10 KEY PREDICTIONS FOR 2011

Also in this issue

BANK INTERNAL AUDIT... THIRD LINE OF DEFENCE OR FIRST LINE OF ATTACK?

Peter Hughes FCA is Director of Internal Audit and Risk at Risk Reward Ltd and a Visiting Research Fellow at the York Management School, University of York. He was formerly a bank Chief Auditor and Head of Risk Management. In this article Peter examines the three lines of defence concept that is widely accepted as risk governance best practice and assesses its implications for internal audit.

The 'three lines of defence' concept has become the widely accepted standard for best practice risk management governance. Banks' internal capital adequacy assessment processes (ICAAPs) invariably feature it as the means of achieving a strong risk culture in their particular organisations.

What are these three lines of defence? Here is not an untypical representation developed specifically for banks:

First Line of Defence
Top Management and Front Office

- Promote a strong risk culture and sustainable risk-return thinking
- Portfolio optimization on the macro and micro level
- Promote a strong culture of adhering to limits and managing risk exposure
- Ongoing monitoring of positions and inherent risks

Second Line of Defence
Risk Management Function

- Combination of watchdog and trusted advisor; police limits with 'teeth'
- Understand how the business makes money and actively challenge initiatives if appropriate
- Top talent with business experience engaging with front office as equals
- Risk management separate from risk control
- Overarching 'risk oversight unit' across all risk types
- Intraday availability for data and positions; comprehensive report at T+1 / 6 a.m.

Third Line of Defence
Audit

- Good understanding of capital markets, the business type, and risk management
- Top talent within audit to challenge the front office and risk management function
- Independent oversight function with enforcement ability (e.g., immediate fulfilment of findings)
- Ability to link business and risk with process and IT know-how

Source: Booz & Co

This three lines of defence concept is about to be set in stone. In a consultative document recently issued by the Basel Committee on Banking Supervision entitled 'Sound Practices for the Management and Supervision of Operational Risk' reference is made to reliance on three lines of defence as common industry practice for sound operational risk governance. These are:

I. Business line management
II. An independent corporate operational risk management function
III. An independent review and challenge

Whereas the paper does not explicitly assign the third level of defence to internal audit this would be the expected configuration in the majority of cases.

The use of the word 'defence' with such prominence when applied to risk governance implies that there is exposure to threats that is both ongoing and unpredictable. In other words, the nature of systemic and related risks exposes banks to unexpected losses that can occur at any time and to any degree. Evidence that this is the case can be found in the financial crisis. Many banks of all sizes had accumulated unidentified and unquantified risks on an unprecedented scale which ultimately triggered losses causing the failure, bailout and nationalisation of banks around the globe that in turn wreaked havoc on national and global economies.

In examining the causes of the financial crisis, in written testimony prepared for the US House of Representatives Financial Services Committee in October 2009, Professor Andrew Lo commented; "Before we can hope to reduce the risks of financial crises, we must be able to define and measure those risks

BANK INTERNAL AUDIT...THIRD LINE OF DEFENCE OR FIRST LINE OF ATTACK?

explicitly. Therefore, a pre-requisite for effective financial regulatory reform is to develop dedicated infrastructure for defining, measuring, monitoring, and investigating systemic risk on a standardized, ongoing, and regular basis."

If an industry and the organisations that comprise it have not yet been able to neutralise threats by resolving the underlying causes then there is little alternative but to construct lines of defence to cushion and contain the actual and potential effects. The increased minimum capital requirements mandated in Basel III in the absence of any risk management based theory or rationale is just one example of effects being addressed rather than their causes. In the case of risk governance, as indicated by Professor Lo above, the neutralisation of systemic and related risks requires the development of 'dedicated infrastructure for defining,

measuring, monitoring, and investigating (them) on a standardized, ongoing, and regular basis'; a capability that is lacking across the financial services industry.

In such periods of ongoing and unresolved threat it is not unusual for functions that possess relevant expertise to assume roles and responsibilities beyond their normal attributes in order to ensure as robust a defence as possible. But such exceptional arrangements only need prevail for as long as the related threats prevail. If threats to risk governance are resolved through the design and implementation of an effective risk identification and measurement framework then the role of risk management, in all probability, will devolve to the maintenance and operation of the framework. Enterprise-wide risk management then becomes the natural response to such a common risk measurement framework provided it has credibility. In the absence of such a framework risk managers are more likely to act as 'watchdogs', 'trusted advisors', 'police with teeth' and 'challengers of initiatives' whereas such attributes are more likely to be associated with audit.

In these unusual times functional boundaries between risk management and internal audit can easily become confused with one function gaining profile to the detriment of the other. Consequently, Chief Auditors, Audit Committees and Chief Executive Officers must remain sensitive to this eventuality and ensure that the role of audit does not lose profile or suffer impairment. After all, whatever the functional boundaries are in practice the accountabilities audit has vis-à-vis the board of directors and various external stakeholders is non-negotiable.

There are real grounds for concern here given that the label 'third line of defence' applied to audit implies subordination to risk management's 'second line of defence'. Indeed, such labels may be inappropriate if the view is taken that the lines of defence concept is transient and only meaningful for as long as there are ongoing and unresolved threats. After all, the three lines of defence concept is not used in conjunction with the relationship between internal audit and the more established and mature functions such as finance management.

Chief Auditors, Audit Committees and Chief Executive Officers should ensure that the roles of internal audit and risk management are examined, evaluated and unequivocally reaffirmed. In this regard a healthier view of internal audit in relation to ineffective risk governance, and one that is more likely to ensure the audit function's effectiveness and optimisation, is 'first line of attack' rather than 'third line of defence'. In this scenario, the primary role of the relatively new discipline of risk management is to complete the creation of the framework that enables the proactive definition, measurement, monitoring and investigation of risks. The primary role of internal audit is to evaluate and challenge emerging solutions and, through its ongoing audit activities, identify and inform senior management and the board of shortfalls between the actual incidence of risk and the framework applied in its identification, measurement and management.

It goes without saying that if internal audit is to be positioned as the first line of attack on inadequate risk governance then it must have the necessary 'top talent' within its ranks and operate state-of-the-art risk-based approaches to auditing.

PJH@riskrewardlimited.com

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

Peter Hughes
telephone: +44 (0)20 7638 5558
email: PJH@riskrewardlimited.com