

Covering the odds

How does the creation of a principles-based regulatory environment affect the role of internal audit? Vicky Kubitscheck shares her thoughts

» PRESCRIPTIVE and specific rules don't work. Events continue to fuel this common assertion, unfortunately. The rogue trader scandal at Société Générale, and the flawed sales and advice procedures around sub-prime mortgages, are just the latest examples. Regulatory regimes can no longer confine themselves to specific rules for governing particular aspects of an organisation, such as product, sales process or financial management. They are extending their reach and taking a "deep dive" approach to evaluating the competence of management.

The UK's Financial Services Authority is widely recognised as taking a lead in this area. The FSA initiated a significant shift in its approach – from being rules-led to one that is based on high-level principles – at the beginning of the century. Yet it is only more recently that the implications of this change are being realised, through record fines and warning shots to firms to get their houses in order.

In a principles-based regulatory environment, the FSA no longer confines itself to specific rules for

supervising firms; it has the ability to challenge all aspects of a business – from strategic planning, decision making, corporate governance, and financial management to operational matters such as information technology, security, business continuity, outsourcing and

“It is only more recently that the implications of this change are being realised, through record fines and warning shots to firms to get their houses in order”

succession planning. With its set of 11 high-level principles, the FSA aims to influence a change in corporate behaviour. (see *High level principles*)

Principles-led regulation is not confined to the UK financial services industry. The provisions of the US Sarbanes-Oxley Act 2002, developed immediately after the demise of Enron,

cover the broad principles of good corporate stewardship, fraud and risk management. Unfortunately, these were overshadowed by the cost of compliance related to Section 404 of the Act and the required attestation of controls over the financial reporting process.

However, the guidance issued by the US Public Company Accounting Oversight Board (PCAOB) and US Securities and Exchange Commission (SEC) since December 2006, aims to redress the balance. We are beginning to see firms refocus more appropriately on the substance of the Act with regard to raising standards of their risk management and systems of internal control within the organisation as a whole.

We also see more reference to principles in the new Basel 2 (2006) regulatory requirements and the European Solvency II proposals under consideration.

Accountability and outcome

With its principles-led approach, the FSA will not be prescriptive. Instead, it focuses on outcomes »



» – the results of management effort and personal accountability.

At the heart of the FSA's principles-based approach is its Approved Persons (APER) regime, which stresses personal accountability, and Senior Management and Systems and Controls Rules (SYSC). Within this framework, internal audit and risk management are Controlled Functions, requiring the individual who leads the internal audit function to be qualified to do the job and be registered as an Approved Person.

The FSA's Treating Customers Fairly (TCF) initiative is a fine example of its principles based approach, requiring firms to determine their own policies and processes to achieve the required outcome for dealing with their customers "fairly". Indeed, firms are expected to define for themselves what "fairness" means – a term that expresses an emotive and changeable human perspective. While processes are essential, what counts will be whether customers feel they have been treated fairly.

Firms who are unable to demonstrate the required outcomes, such as fair treatment of customers or a secure environment for their investments, will be held accountable – where appropriate, on a personal basis under the Approved Persons regime.

The upside of a principles-based regulatory environment with less prescription, according to the FSA, is that industry-led solutions and best practices will emerge, encouraging innovation and healthy competition.

Raising the bar

The scene is set for top management to rise to these higher challenges. But is "raising the bar" for higher standards of governance and assurance sufficient in a principles-based regulatory environment? With a decreasing appetite for failure and risk of reputation damage, the need to cover all the odds by adopting a risk- and principles-based approach might just make the mark.

The internal audit profession is no stranger to a principles-based approach

High level principles

The FSA says that a financial firm must:

- 1 Conduct its business with integrity.
- 2 Conduct its business with due skill, care and diligence.
- 3 Take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
- 4 Maintain adequate financial resources.
- 5 Observe proper standards of market conduct.
- 6 Pay due regard to the interests of its customers and treat them fairly.
- 7 Pay due regard to the information needs of its clients, and communicate information to them in a way that is clear, fair and not misleading.
- 8 Manage conflicts of interest fairly, both between itself and its customers and between a customer and another client.
- 9 Take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgment.
- 10 Arrange adequate protection for clients' assets when it is responsible for them.
- 11 Deal with its regulators in an open co-operative way, and must disclose to the FSA appropriately anything relating to the firm of which the FSA would reasonably expect notice.

to regulating behaviour. The IIA's *International Standards* and *Code of Ethics* are based on principles rather than a set of rules. Indeed, there is significant alignment between the FSA's High Level Principles for management and the IIA's *International Standards* and *Code of Ethics*. For example, the FSA's Principles 1, 2 and 3 state that:

- A firm must conduct its business with integrity (IIA Principle 1: Integrity)
- A firm must conduct its business with due skill, care and diligence (IIA Principle 2: Skill, care and diligence)
- A firm must take reasonable care to organise and control its affairs reasonably and effectively, with adequate risk management systems (IIA Principle 3: Management and Control)

So, how are internal auditors rising to the challenge and covering the odds of potential financial and reputation ruin of their organisations? How are internal auditors aligning themselves with the efforts of management? How

"The internal audit profession is no stranger to a principles-based approach to regulating behaviour"

are internal auditors disclosing non-compliance with these principles?

Creative internal audit

With the shift towards required “outcome” – or in internal audit language, the validated effect of management action – the internal auditor should be on familiar territory. The auditor is trained to focus on the objective of an action or mitigating control.

The attention on outcome allows flexibility and creates opportunities for firms to be innovative and competitive in delivering solutions that are aligned to their unique business models. For the internal auditor, significant opportunities arise to display their core skills and business acumen while adding real value to management.

To do this, the internal auditor must first understand the challenges facing the organisation. For example, as industry-led solutions become the standard, firms need to adopt a more dynamic approach to reviewing their business and behavioural frameworks against peer groups to maintain a state of compliance, as well as their competitive position. Furthermore, in the absence of detailed rules, firms will be required to determine for themselves minimum standards and policies for delivering their products and services, as well as for conducting themselves.

Internal auditors who are well armed with this understanding can better support and respond to the needs of management in accordance with the firm’s appetite and capacity for risk. In particular, internal audit should ensure that it develops a

capability to think broadly, creatively and ahead. Failure to do so could result in internal audit being side-lined – to be relegated to mere checkers or be replaced, whether internally or externally, as management is forced to seek support from other sources.

Repositioning internal audit in an outcome-focused, risk- and principles-based regulatory environment involves three main steps:

First, establish a more critical understanding of the root causes of a control failure or near miss, before rushing to make a recommendation.

Second, develop integrated solutions that minimise duplication and cost by understanding the operating models deployed by the business. This involves working closely with other risk-related functions, such as the finance, risk and compliance areas.

Third, develop capability that promotes innovation and creativity in the way internal audit plans, identifies and evaluates controls. Controls must be effective in managing the wide spectrum of risks to the business. Controls that add value are those that are balanced in achieving the compliance and performance objectives of the organisation. The internal auditor is required to think more strategically than ever before, while ensuring a focus on outcomes that matter.

While the IIA’s principles of internal auditing continue to provide a sound basis for supporting top management, the manner in which they are applied must evolve. Internal auditors appreciate that risks to an organisation are unavoidable. However, the new risks arising in a principles-based regulatory environment can be limited if management and the internal audit function adopt the right approach. ●

Vicky Kubitscheck is a partner at Independent Audit and chair of the Insurance Internal Audit Group. vicky.kubitscheck@independentaudit.com. This article is based on a case study she wrote for *Cutting Edge Internal Auditing*, a book by Jeffrey Ridley



Ad
page
31