



THE ROLE OF INTERNAL AUDIT - A PRUDENTIAL PERSPECTIVE

JOHN F LAKER

Chairman
Australian Prudential Regulation Authority

*The Institute of Internal Auditors-Australia, NSW Chapter
Sydney*

THE ROLE OF INTERNAL AUDIT - A PRUDENTIAL PERSPECTIVE

Introduction

The internal audit function is one of the fundamental “checks and balances” for sound corporate governance. Now more than ever, a robust and objective internal audit function, with the skills to identify risk control problems and the authority to pursue its concerns, is essential to the proper discharge of directors’ responsibilities. It is, as well, a firm ally of the prudential regulator. For this reason, I welcome the opportunity to address the NSW Chapter of the Institute of Internal Auditors and offer an APRA perspective on the role of internal audit in our supervised institutions. I understand this is the first occasion that APRA has addressed the Institute at this level and I hope this augurs well for a growing relationship between the Institute and APRA.

Corporate governance, as we all know, has been under a strong and critical public spotlight in recent years, in the wake of a succession of blows to market confidence and integrity, particularly in the United States but echoed in Australia and other countries as well. The community’s expectations of boards and senior management, and of those charged with providing an independent review of a company’s operations and financial accounts, have been raised. To meet those expectations, governments and regulatory authorities around the globe have mounted a concerted campaign to improve standards of corporate behaviour and transparency through the international harmonisation of accounting standards, strengthening the principles of corporate governance, lifting the bar on the “fitness and propriety” of directors and managers and introducing improved market disclosure standards.

In this demanding environment, boards and senior management need quality advice from sources that can be trusted and that can offer an objective viewpoint. Much of the focus of Sarbanes-Oxley in the United States and CLERP 9 in Australia has been on the external audit function. Equally, however, there is a need to ensure that internal audit is organised, resourced and empowered so that it can provide competent, impartial and fearless advice. In contrast to external auditors, however, our sense is that internal audit is still evolving as a profession and has further to go in promoting its own professional standards and profile in Australia. We in APRA observe that internal audit in our supervised institutions is not based on widely utilised standards, recognised by Audit Committees for example, and it is not always focussed on the same set of issues. Internal audit functions vary from a narrow concern with compliance or financial accounts to a broader remit reviewing efficiency and effectiveness or acting as an internal consultant.

My address today offers a prudential perspective on the role of internal audit. It starts with the separate roles of internal audit and risk management in the corporate governance framework. It then sets out the expectations of internal audit held by prudential regulators at the international level and how APRA assesses whether internal audit in the institutions it supervises meets these expectations. Finally, I discuss some particular internal audit issues. My comments are offered in a constructive spirit to encourage debate within the internal audit profession, and they draw on the “fields of fire” experience of key staff who have joined APRA from internal audit roles in industry.

The role of internal audit

What better starting point for my comments than the definition of internal audit approved by the Board of Directors of your Institute:

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

I remind you of this definition because I want to draw a distinction between internal audit and risk management. As we see it, the basic function of internal audit is independent appraisal of an institution’s internal controls, including controls over financial reporting. Simply put, it is about reviewing activities to ensure that they are carried out as intended. Of course, a by-product of internal audit will be recommendations on internal control and process improvements that could be made, an important role for internal audit in large and complex financial institutions in particular.

Risk management, on the other hand, is about identifying and assessing inherent risks in the products and activities of an institution, and ensuring that appropriate risk management limits, control mechanisms and mitigation strategies are in place to contain risk within the institution’s risk appetite and capital support. It is critical in helping an institution plan its strategic response to its changing risk profile and ensuring effective risk management processes are in place to respond quickly. Yes, a checking function (similar to internal audit) is often involved to ensure that the risk control framework is in place and operating as intended; internal audit also plays a complementary role in evaluating whether the controls are practical, whether they are functional and how they might be circumvented. The distinction is that risk management has the important and continuous responsibility of understanding how actual risk facing the institution is changing (day-by-day or month-by-month) and assessing if the risk limits, controls or mitigations need updating.

Of course, institutions need to ensure cooperation between internal audit and risk management and a clarification of roles, so that unintended gaps do not emerge. For example, as new procedures are put in place to address emerging risks, the risk management function needs to keep internal audit informed and, vice-versa, if internal audit identifies any weakness or gaps in the application of risk controls.

The expectations of prudential regulators

The pivotal role of internal audit in the corporate governance of financial institutions is enshrined in international standards for prudential regulators, though they are high-level in nature.

In banking, the *Core Principles for Effective Banking Supervision*, developed under the auspices of the Basel Committee on Banking Supervision, specifies the principle that banks should have in place internal controls that are adequate for the nature and scale of the business. These should include, *inter alia*, appropriate independent internal or external audit and compliance functions to test adherence to these controls as well as applicable laws and regulations.

In assessing adherence to this principle, the Basel Committee's "essential criteria" for the internal audit function is that it:

- have unfettered access to all the bank's business lines and support departments;
- have appropriate independence, including reporting lines to the board of directors and status within the bank to ensure that senior management reacts to and acts upon its recommendations;
- have sufficient resources, and staff that are suitably trained and have relevant experience, to understand and evaluate the business it is auditing; and
- employ a methodology that identifies the key risks run by the bank and allocates its resources accordingly.

The language of the *Insurance Core Principles and Methodology*, developed under the auspices of the International Association of Insurance Supervisors (IAIS), is almost identical on the role of internal audit in insurance companies.

The Basel Committee also issued a paper, *Internal audit in banks and the supervisor's relationship with auditors*, in August 2001 to provide more detailed guidance to bank supervisors. The paper has wider applicability and I commend it to those who are not familiar with it. It sets out 20 separate principles for the internal audit function, dealing with such issues as continuity, professional competence, the audit charter and relationships with the external auditor. I would draw attention to two particular principles:

- the internal audit function must be independent of the activities audited and independent from the every day internal control process. This means that internal audit is given an appropriate standing and carries out its assignments with objectivity and impartiality; and
- every activity and every entity of the institution should fall within the scope of the internal audit.

I would note, in passing, that this breadth of scope should ensure that the internal audit function adds value to the institution, its board and its senior management.

APRA's assessment of internal audit

APRA fully endorses the principles of the Basel Committee and the IAIS on internal audit.

In the case of authorised deposit-taking institutions, our prudential standards require that locally incorporated ADIs have a comprehensive and independent internal audit process for reviewing and testing their internal controls and risk management systems. The scope of the internal audit should include a review of the processes and controls put in place by management to ensure compliance with APRA's prudential requirements. Where the scale of an ADI's operations does not justify maintaining a full-time internal audit function, the ADI should agree alternative review arrangements with APRA.

In general insurance, our Discussion Paper on Stage II reforms released last November proposed that internal audit requirements identical to those for ADIs be

incorporated into prudential standards for general insurance companies. The notice of a dedicated internal audit function has found considerable industry support. The Discussion Paper also proposed that internal audit report directly and solely to the Audit Committee (or board), a proposal I will discuss later. In life insurance, internal audit requirements are set in the *Life Insurance Act 1995* rather than in prudential standards, and they are limited to the requirement that the records of a life company be audited and that the life company have an audit committee comprised of directors, or a non-director if approved by APRA.

Beyond these high-level prudential requirements, APRA has not as yet provided detailed guidance to regulated institutions about the internal audit function. However, APRA does make its own assessment about the quality of internal audit as part of a formal process for risk-rating institutions, and you will get a strong sense of our approach if I share with you, in broad terms, how we undertake this assessment. Our approach recognises that internal audit functions vary according to the nature and complexity of institutions and it is not "one size fits all". Careful judgment is required.

Our starting point is determining whether the internal audit function is in-house or outsourced, and whether this arrangement is appropriate. You will recall that an institution needs to agree alternative review arrangements with APRA if a full-time internal audit function cannot be justified. Our supervisors then review the following features of the internal audit:

(i) Structure and resources

The structure of the internal audit function is established and an assessment made about the key internal audit personnel, their roles and responsibilities, skills and experience. Where the function is outsourced, the focus includes the terms of the outsourced arrangement and how this is monitored.

(ii) Independence

The board of the institution should ensure that the independence of the internal audit function is maintained. This independence may be compromised if the function is directly involved in risk management or operational processes. The internal audit function may provide valuable input to those responsible for risk management but should not itself have direct risk management responsibilities. In practice, some institutions (particularly small ones) may give internal audit initial responsibility for developing a risk management program. Where this is the case, institutions should see that responsibility for day-to-day risk management is transferred elsewhere in a timely manner. Where the internal audit function is outsourced there should not be any conflicts of interest - for example, internal audit should not be a source of referral business for the institution.

(iii) Approach

This approach taken by internal audit should be clear and may be one or a combination of:

- risk-based - the focus is on the high-risk areas of the institution;
- review-based - the focus is on reviews of various parts of the institution, usually chosen both at random or in line with the internal audit plan; and/or

- compliance-based - the focus is on compliance with policies and procedures.

The board should have endorsed the approach and there should be sufficient scope to change it where necessary, in order to react quickly to issues that arise requiring internal audit involvement.

(iv) Internal audit plan

The internal audit plan, which usually details the proposed internal audit work for the next 12 months, should be documented and endorsed by the board. Importantly, the plan should be consistent with the type of approach to be taken and should be adequate for the scale and complexity of the institution's operations. In assessing the robustness of the plan, our supervisors focus on:

- whether there is a dedicated **planning process** for the development of the plan. The plan should not simply be the responsibility of the internal auditor for "rubber-stamping" by the board. The board, Audit Committee and management must ensure the plan reflects the needs of the institution;
- whether the plan clarifies the **objectives, scope and cycle** of internal audit, which the head of internal audit should be able to explain in detail;
- whether the **external audit** has highlighted areas of weakness in the internal control environment that require internal audit review; and
- whether **progress against the plan** is monitored regularly by the Audit Committee and reported to the board.

(v) Reporting

Although not a formal prudential requirement, APRA expects the head of internal audit to report findings to the Audit Committee (or board) regularly. Serious issues should be elevated to senior management and the Audit Committee (or board) without delay. Issues should be monitored to ensure that appropriate action is being taken in managing the risk and that the possibility of loss, financial or otherwise, is appropriately mitigated. The head of internal audit should have unfettered access to members of the Audit Committee (or board) as and when required. The head of internal audit should report to the Board if internal audit experiences irresolvable difficulties in attempting to conduct a review in a business area because of non-cooperation or hindrance by management.

More generally, there should be a clear flow of reporting from internal audit to the Audit Committee and board. Reports should clearly show the frequency of reporting; they should focus on the internal audit work performed and issues arising within the required period, and whether work is in line with the plan. Reports should also detail, where appropriate, any emerging risk issues that are proposed for internal audit involvement.

APRA also expects the external auditor to be provided with relevant reports and papers as necessary. The internal auditor should liaise with the external auditor on a regular basis, and particularly where there are significant control issues that the external auditor should be aware of or that may impact on the assessments made during the financial statement audits.

Some internal audit issues

This overview of APRA's approach to assessing internal audit cannot, of course, convey the colour and complexity of some of the internal audit issues with which we deal. I would like to offer you our thoughts on some of these issues:

(i) Establishing the authority of internal audit

In APRA's view, the internal audit function needs to have strong standing within the institution. It must be recognised as a core part of governance and not as some form of necessary burden or add-on. Asserting the importance of authority is one thing, earning that authority is another. In the end, it is the professionalism and quality of internal audit work that will show boards, senior management and regulators that the function does add value. Clearly, the message that internal audit wants to send will not carry weight if it cannot demonstrate that the message is founded on both technical and commercial competence - a balancing of technique and "real world" skills and experience.

Internal audit can seek to boost its authority within the institution in a number of ways. A critical challenge is to strengthen the competencies of internal audit staff. These days, internal audit needs to adopt a strategic orientation, to undertake a range of complex audits and to match the speed with which risks can emerge in the institution. To do so, the skill mix needs to be a broad one, embracing accounting, expertise in compliance checking, specialist treasury and IT skills and strategic thinking. Other ways to boost authority include:

- ensuring that internal audit is adequately funded;
- where necessary, 'in-sourcing' additional specialist skills to supplement full-time audit resources;
- ensuring that internal audit technology keeps pace with developments in the business; and
- demonstrating professionalism and objectivity by standing up against management and others, when this is justified in the interests of shareholders, beneficiaries and the public. I will say more on this point below.

Fundamental to authority is the attitude and thinking which internal auditors bring to their work. The strength and calibre of internal auditors themselves. These qualities need to be nurtured through active selection and training programs and well-established career progression in internal audit. We wonder, as well, whether internal auditors will be more empowered if they think of internal audit as a profession in its own right, supported by this Institute, rather than as some type of stepping stone into corporate management.

(ii) Transparency and independence

In APRA's view, the provision of independence assurance to the Audit Committee (or board) is the central tenet of internal audit. Consistent with this view, our Discussion Paper on Stage II reforms to general insurance proposed that the internal audit function should report directly to the Audit Committee of the board, and not to management with operational responsibilities. A direct reporting line to the board has now become international best practice.

This proposal has attracted a considerable degree of resistance. A number of respondents have argued against a sole reporting line to the Audit Committee (or board) as being beyond current Australian best practice. The claim is that there are good practical reasons why internal audit should report to senior management for day-to-day oversight. One of these is the growing reliance of senior management on the skills and knowledge of internal audit staff for consultation purposes, in addition to traditional audit services. That may be so, but its role in governance should take precedence over other internal audit activities.

In our view, having internal audit answer to management creates real concerns about the independence of the review function. These concerns are magnified when that reporting is to the Chief Finance Officer rather than the Chief Executive Officer - there is an inherent conflict where all financial management, internal and external audit converge into one area of responsibility. Internal audit must be able to directly inform the Audit Committee (or the board) about the adequacy or otherwise of internal controls, including those involving high-level management. Internal audit must know that the board is its master.

Although we have yet to finalise the general insurance reforms, APRA holds to the view that, as a minimum, there should be direct, two-way access between internal audit and the Audit Committee (or board). This direct line of reporting is needed to ensure that internal audit gets its message through without any filtering by senior management. Obviously, in responding to internal audit's recommendations, the Audit Committee (or board) would consult with management, and seek outside advice if appropriate. But the response must be from the Audit Committee (or board), not management.

We would also expect the Audit Committee (or board) to receive full internal audit reports. Sometimes only short summaries of final reports are provided. These may not reveal issues identified in preliminary reports that were subsequently rectified by management. In the course of our supervisory reviews, we have also noted many examples where internal audit has uncovered issues that have remained outstanding for long periods of time (sometimes indefinitely) for want of management attention. This sort of track record would also surely be of interest to the Audit Committee.

In the end, of course, effective escalation involves more than procedures and reporting lines; it has very much to do with an open and transparent organisational culture. The best test of an effective escalation procedure is how the board and senior management react to the receipt of "bad news". Experience suggests one of the main reasons why Audit Committees fail is that they do not get to hear about the risk issues that matter.

(iii) Relationship with external audit

As APRA's own assessment procedures confirm, the relationship between internal audit and the external auditor is very important. In some areas, the external auditor will rely on the work of internal audit, and this requires an open and cooperative relationship between both functions, with a clear delineation of responsibilities. An equal partnership, where that can be achieved. While external audit is largely focussed on the financial statements, prudential requirements are pushing some broader responsibility onto the external auditors. However, this is aimed mainly at general whistle-blowing and sign-offs that specific tasks (nominated by the regulator) have been carried out as expected. This expanded

role will never replace the need for an effective internal audit function as a broad control and review mechanism in institutions.

(iv) Audit Committees

The effectiveness of internal audit comes down, ultimately, to the use that the Audit Committee and board decide to make of it. These days, diligent and probing board directors want a strong and active internal audit function to assist them. They rely on internal audit's knowledge of the risks facing the institution and the control weaknesses, and its recommendations for improvement, to help them discharge their responsibilities. If that is not occurring, a professional internal audit function and its head should be saying so. This goes to the heart of the professionalism of internal audit staff.

For the Audit Committee itself to be effective, it needs to:

- understand the system of internal controls used to monitor and manage risks;
- consider whether internal control recommendations are being implemented by management; and
- require the Board to make the necessary changes.

The Audit Committee faces a particular set of challenges when the institution is part of a global group. In these cases, the audit function (external and internal) is normally subject to group expectations and direction. Priorities and focus are on a global basis and Australian activities may not receive the priority they might otherwise. Materiality levels are also normally much higher at a group rather than a subsidiary or branch level, and this can mean that issues for the Australian entity may not be subject to appropriate levels of scrutiny.

(v) Conflict situation

Prudential regulators can cite too many examples where weak corporate governance has undermined the financial soundness of an institution, whether through unfocused global expansion, pursuit of growth for growth's sake, a dominant chief executive officer or a "good news" syndrome. Internal audit should be alert to such signs of weakness and raise them with the Audit Committee (or board) as governance, controls or review concerns. APRA views very positively an internal audit function that is active in discovering compliance weaknesses and that escalates these for remedial action. No financial institution ever has in place internal controls that are beyond fault; there are always improvements to be made.

Ultimately, it is the board which has to take ownership of problems and institute appropriate remedies. And what should internal audit do where its institution is facing major problems and no notice is being taken? There is no easy answer, since each situation is unique. Nonetheless, it is surely incumbent on internal audit staff to take the right professional action and not let the situation fester. In the end, the head of internal audit might have to resign if the institution's culture does not allow internal audit to function appropriately and serious problems are not being addressed. This is the ultimate test of the professionalism and ethics of internal auditors, and we would presume that their long-term professional reputation would be more important than their current employment situation.

This may seem easy for a prudential regulator to say and we acknowledge that it is very lonely for a professional to be in such a dilemma. After any failure, however, internal audit is inevitably one of the sacrificial lambs on the altar of accountability, and internal auditors do well to remember that if they are being tempted into silence or acquiescence. In these difficult situations, professional standards and support from the professional body can help to strengthen the position of the internal auditors involved. APRA has required external auditors and actuaries to whistleblow to the regulator in extreme circumstances, while granting them protection in the form of qualified privilege. We may need to consider similar arrangements for internal audit staff.

Concluding remarks

The ever-increasing pressure on institutions to manage their affairs and risks prudently poses considerable challenges for corporate governance structures and for internal audit, a key line of defence in these structures. Every challenge, however, is an opportunity. For internal auditors as a profession, the current environment is an opportunity to cement your presence in corporate Australia. The work of this Institute in strengthening professional standards and education could not be more timely and it has our full encouragement.

For internal auditors at the coal-face, you have the opportunity - more than that, the obligation - to demonstrate your skills, your nous and your resolve in the vital role you play. You have more than our full encouragement, you have our full support. For our part, our expectations of internal audit in APRA-regulated institutions are being clarified and strengthened in prudential standards. We have also been emphasising, publicly and privately, that institutions need to maintain their expenditure in risk management systems and resources, including internal audit, and that this vital infrastructure should not be a candidate for short-sighted cost cutting.

The challenges and opportunities for internal audit in this risk-focussed environment can perhaps be simply summarised as "looking at the right things, not just doing things right".