vmia
Risk Management and Insurance

WHAT IS INTERNAL AUDIT?

August 2017

VICTORIA
State
Government

Contents

What is Internal Audit?

1. Is internal audit mandatory?

In short, yes – an internal audit (IA) function is mandatory for all organisations that come under the Financial Management Act. The Standing Directions of the Minister for Finance 2016 (under the Financial Management Act 1994) specify a range of responsibilities for the IA function, including preparation of a charter and strategic plan. Further, an organisation's responsible body is required to establish an audit committee to "independently review and assess the effectiveness of the Agency's systems and controls for financial management, performance and sustainability, including risk management".

2. What is the difference between internal and external audit?

As defined by the Institute of Internal Auditors, IA is an "independent, objective assurance and consulting activity designed to add value and improve an organization's operations". In simple terms, IA provides the board with the assurance that the organisation's risks are being appropriately managed, the risk controls in place are working well and there is adequate management oversight.

The IA function may be executed by an in-house team of auditors and subject matter specialists. This function may also be outsourced to a professional auditing firm. Even though this firm is external to the entity they are auditing, they are still known as the internal auditors. The IA function may also be co-sourced between an internal and external provider. This has advantages for developing strong relationships and engagement between IA and management, which is key to the successful operation of an IA function.

On the other hand, the role of external audit is to evaluate the integrity of an entity's financial systems when assessing the accuracy of the entity's financial statements. The external audit service must be obtained from a professional accounting firm who is sourced from outside the organisation they are reviewing.

The internal and external audit functions are complementary in nature. Whilst the functions operate independently, they will share information in order to maximise efficiency, reduce costs and avoid unnecessary impact upon the area under review.

3. How is an IA review performed?

There are four key steps for conducting an IA review:

i. **Develop an audit plan:** The IA plan usually includes a 12 month program of work and a 3-4 year forward plan that outlines the areas of risk that will be reviewed. Better practice IA plans are built on a number of key principles:

   a. Firstly, the plan should be risk based. That is, it reflects the governance arrangements, risks and control measures that make up the organisation's risk profile. The plan should reflect the organisation's strategic objectives, compliance obligations and the requirements of its regulators.

   b. Secondly, the plan should be a top-down and bottom-up reflection of the priorities and matters of potential concern to the board and management. It is essential to have buy-in from these key stakeholders to help allocate IA resources into areas where they are most wanted and needed.

   c. Thirdly, the plan needs to stay relevant. The plan should be periodically reviewed to ensure it adequately addresses risks attributable to the organisation's changing operating environment, strategic objectives and priorities.

ii. Planning/scoping: This is a determination of the actual risk areas to be considered and the approach the IA team will take for conducting the review. This is usually achieved through discussion with management to understand the key risks, controls and operating processes in the area under review. This includes identifying matters of concern to management that would benefit from an independent assessment. This way, management has input into the value they can attain from the audit and the assurance they require. Ultimately though, the audit is performed to meet the board's expectations and needs for assurance.

During scoping, the IA team will likely request certain documentation from management to help them build an understanding of the area under review, including the strategic and performance objectives, policies, and operating procedures. The timing of the audit will also be agreed upon to ensure key staff are available during fieldwork and that critical times in the organisation's operations are not unduly interrupted. The scope and approach are usually agreed in advance with management and the audit committee, 1-4 weeks prior to audit fieldwork commencing.

iii. Fieldwork: This phase is an assessment of the design and effectiveness of risk controls, operating processes and the adequacy of oversight and governance arrangements. This may be achieved through discussions with management and staff, control re-performance in a test environment, observation of controls operating in a live environment, or through analysis of historical data.

iv. Reporting: The outcomes of reviews are communicated through a written report that is shared with the audit committee and management. In an assurance review, the report will include an opinion about the adequacy of the governance, risk management and control measures in the area under review.

The report may include commentary on the strengths observed in operating processes as well as audit issues. These are descriptions of activity that is occurring outside of the expected operating environment. This may be a control that is not working as expected, a risk that doesn't have adequate controls to mitigate the risk to an acceptable level, or where there is insufficient oversight over the operating environment. Issue wording includes specific actions that management will perform to treat the issue, which are tracked to completion by the IA team and audit committee.

In the event that no matters have arisen, a "clean" audit report may be issued. A clean report could still include a benchmark of the entity's activity against better practices, or a comment in relation to the entity's overall risk culture, which can provide further insight of value to management.

In an advisory review, IA will provide advice and opinion on matters such as functional design, control design, efficiency, systems and better industry practices. The report will often be in a similar format to the assurance review, although the matters identified will likely be recommendations rather than issues requiring management actions.

4. What rigour is there in an IA review?

All internal audits must be conducted in accordance with the International Professional Practices Framework (IPPF) which is published by the Institute of Internal Auditors. The IPPF includes strict requirements around ethics, independence, objectivity and performance. In simple terms, this means that internal audit opinions must be a reflection of facts that are based on the best available evidence and obtained through the approved IPPF methodology.

Victorian public sector organisations must have a charter that confirms the IA function's independence from management and permits them access to any people, processes, systems or premises necessary to perform an IA review. The IA function reports directly to the board audit committee (or similar), who oversee the deliverables and quality of the IA program.

5. Will the IA team know anything about my organisation?

Yes. It is critical that the IA team has the right people looking at the right risks.

People: The basis of a good IA team is getting the right mix of subject matter expertise and internal audit expertise. Subject matter experts (SME's) are often a key part of an IA team as they have detailed knowledge of the function under review: they understand the operating environment, the key challenges and have seen examples of better operating practices. SMEs will target the right areas to review, ask the pertinent questions and analyse the significance of matters observed. The SME will work alongside the auditor whose role is to ensure that audit methodology is followed, the best available evidenced is obtained, supporting work papers are all in order and the written report offers insight, foresight and clearly worded issues.

Risks: Integrating risk into the IA plan is a key concept for audit value and effectiveness. At a high level, the IA plan is based on the entity's risk profile and the priority areas of management and the board. At a detailed level, the audit scope document is developed by the SME, the IA team and operational management, and specifies the actual processes and areas of risk that will be reviewed.

6. How will I get value from the IA program?

The IA plan is ultimately owned by an entity's board who is generally looking for:

- Assurance that the current risk management, control and governance processes are appropriately designed and operating effectively; and
- Where identified, there are appropriate actions to mitigate control gaps or implement process improvements.

The audit may also detect fraud, corruption or other irregular activities, or identify behaviours that exist outside of the entity's preferred culture. Prevention of such adverse activity is likely to be high on management's agenda for the successful achievement of their business objectives. Getting an independent perspective on such matters may, as is often stated, help them sleep better at night.

Further, where issues are identified, the audit report can be used to raise the profile of a risk requiring treatment and to support management's request for resources to improve risk control measures.

7. What do I need to do in an IA review?

IA resources can be sourced from a professional accounting firm. It is critical that management works with the IA function to:

- Allocate sufficient time to the review. This includes time to meet and discuss matters with the IA team, assist in enquiries, review and provide feedback on draft report wording;
- Provide access to all records, assets, personnel and premises required to for the IA team to fulfil their responsibilities;
- Engage in open, honest and transparent discussion; and
- Cooperate and provide unfettered assistance in a timely manner.

After all, the IA team's time comes at a cost, so an efficient audit is a good audit.

8. Why I shouldn't be concerned about an internal audit in my area

Internal audit IS:	Internal audit IS NOT:
An assurance and advisory function	A 'finger-pointing' exercise
Independent of management	Wielding green pens
Governed by the IPPF	A risk or control owner
Objective in its work	Responsible for managing your risks
Helping an organisation to manage its risks	Part of your control framework
	The only way to get assurance

There are some myths to dispel about IA. In days gone by IA was often seen as the people you hid things from, cleaned up your files for, answered only what was asked of you, or was the team that you avoided at all costs. However, ***IA is not*** the police and is not here to point fingers, pick faults or make you look bad. Furthermore, ***IA is not*** responsible for your risk and control framework and ***is not*** the only place for assurance.

Fortunately, people's understanding and perspectives of IA have shifted over the years and kept pace alongside contemporary auditing practices. There is now a better understanding that ***IA is*** here to ***work with management*** and ***help the organisation*** to manage its risks. To achieve this, ***IA can*** advise on what is working well, ***can*** identify opportunities for improvement, and ***can*** offer insights to help improve operating practices.

9. Key message

Value creation in internal audit is all about relationships: work together with your stakeholders in a partnership, keep the communication lines open, talk frequently and build 2-way trust. It's the simple recipe for value and success.