information and privacy commission
new south wales

Internal audit manual

June 2011

Table of contents

1 INTRODUCTION

1.1 Background

Treasury Circular NSW TC 09/08 implements a new "Internal Audit and Risk Management Policy". The policy aims to ensure that NSW agencies maintain organisational arrangements that provide additional assurance, independent from operational management, on internal audit and risk management.

To achieve this, the policy mandates a set of 'core requirements' that agencies must implement for consistent application across the government sector. The Information and Privacy Commission (IPC) will implement the Treasury requirements to the extent that they can be applied.

The core requirements comprise key governance practices that ensure the real and perceived independence of the Audit and Risk Committee, the Chief Audit Executive and the Internal Audit function, as well as the adoption of current standards for professional practice in internal audit and risk management.

The six core requirements comprise:

- Core Requirement 1: Internal Audit Function – this covers the requirement to establish and maintain an Internal Audit function
- Core Requirement 2: Audit and Risk Committee – this covers the requirement to establish and maintain an Audit and Risk Committee
- Core Requirement 3: Independent Chairs and Members – this covers Committee composition, and the requirement to appoint an independent chair and a majority of independent members
- Core Requirement 4: Model Charter and Committee Operations – this covers the requirements to maintain governance arrangements that ensure both the real and perceived independence of the Committee and the rigour and quality of its oversight and monitoring role
- Core Requirement 5: Risk Management Standards – this covers the requirement to implement a risk management process that is appropriate to the needs of the department or statutory body and consistent with the current risk standard, i.e. AS/NZS ISO 31000: Risk Management – Principles and Guidelines
- Core Requirement 6: Internal Audit Standards – this covers the requirement to ensure that operation of the Internal Audit function is consistent with the relevant standard, i.e. IIA International Standards for the Professional Practice of Internal Auditing and any additional practice requirements set by the Policy.

Consistent with better practice corporate governance principles, the new policy requires agency heads and governing boards of statutory bodies to attest compliance with the core requirements annually, and to provide this information in a new annual report disclosure.

Treasury Policy & Guidelines Paper TPP 09-05 contains procedures for the implementation of the core requirements of the policy. Section 6.7 of that Paper requires the development and maintenance of an Internal Audit Manual for the Internal Audit function. This document constitutes the IPC's Internal Audit Manual in compliance with that requirement.

1.2 Purpose

The purpose of this manual is to:

- delineate basic principles that represent the practice of internal auditing within the IPC;
- provide a framework for performing and promoting a broad range of value-added internal auditing;
- establish the basis for the evaluation of internal audit performance; and
- foster improved organisational processes and operations.

1.3 Scope

This manual applies across the entire organisation of the IPC including any controlled entities, into the future. It addresses both assurance services as well as consulting services provided by the Internal Audit function.

Assurance services involve the internal auditor's objective assessment of evidence to provide an independent opinion or conclusions regarding its operations, functions, processes, systems, or other subject matter. The nature and scope of the assurance engagement are determined by the internal auditor. There are generally three parties involved in assurance services: (1) the person or group directly involved with the IPC's operation, function, process, system, or other subject matter – the process owner, (2) the person or group making the assessment – the internal auditor, and (3) the person or group using the assessment – the user.

Consulting services are advisory in nature, and are generally performed at the specific request of an authorised IPC staff member. The nature and scope of the consulting engagement are subject to agreement with the requesting IPC staff member. Consulting services generally involve two parties: (1) the person or group offering the advice – the internal auditor, and (2) the person or group seeking and receiving the advice – IPC. When performing consulting services the internal auditor should maintain objectivity and not assume management responsibility.

This manual is consistent with the professional practices set out in the Institute of Internal Auditors (IIA) Standards and was endorsed by the IPC Audit and Risk Committee on 15 June 2011 and approved by the Commissioner on 15 June 2011.

2 GENERAL POLICIES AND STANDARDS

2.1 Internal Audit Charter

2.1.1 Introduction

The IPC has established the internal audit function as a key component of its governance framework.

The Internal Audit Charter (see Attachment 1) provides the framework for the conduct of the Internal Audit function in the IPC and has been approved by the Commissioner on the advice of the Audit and Risk Committee.

2.1.2 Purpose of internal audit

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

Internal audit provides an independent and objective review and advisory service to:

- provide assurance to the Commissioner, and the Audit and Risk Committee, that the IPC's financial and operational controls, designed to manage the organisation's risks and achieve the entity's objectives, are operating in an efficient, effective and ethical manner, and
- assist management in improving business performance.

2.1.3 Independence

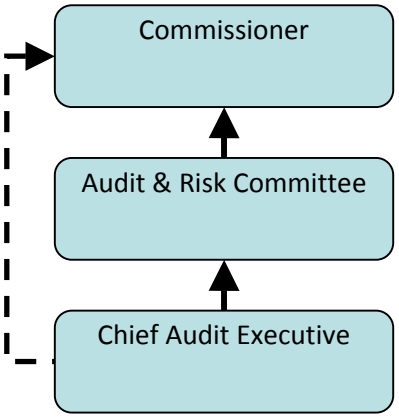
Independence is essential to the effectiveness of the internal audit function. Internal audit activity must be independent, and internal auditors must be objective in performing their work. Internal auditors must have an impartial, unbiased attitude and avoid any conflicts of interest.

The internal audit function has no direct authority or responsibility for the activities it reviews. The internal audit function has no responsibility for developing or implementing procedures or systems and does not prepare records or engage in original line processing functions or activities.

The internal audit function is provided to the IPC on an outsourced basis by a third party provider and is responsible on a day-to-day basis to its Chief Audit Executive.

The internal audit function, through the Chief Audit Executive, reports functionally to the Audit and Risk Committee on the results of completed audits, and for strategic direction and accountability purposes, and reports administratively to the Commissioner to facilitate day-to-day operations.

The following reporting line is prescribed:



2.1.4 Authority and confidentiality

Internal auditors are authorised to have full, free and unrestricted access to all functions, premises, assets, personnel, records, and other documentation and information that the Chief Audit Executive considers necessary to enable the internal audit function to meet its responsibilities.

All records, documentation and information accessed in the course of undertaking internal audit activities are to be used solely for the conduct of these activities. The Chief Audit Executive and individual internal audit staff are responsible and accountable for maintaining the confidentiality of the information they receive during the course of their work.

All internal audit documentation is to remain the property of the IPC, including where internal audit services are performed by an external third party provider.

2.1.5 Roles and responsibilities

The internal audit function must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

In the conduct of its activities, the internal audit function will play an active role in:

- developing and maintaining a culture of accountability and integrity
- facilitating the integration of risk management into day-to-day business activities and processes
- promoting a culture of cost-consciousness, self-assessment and adherence to high ethical standards.

Internal audit activities will encompass the following areas:

(a) <u>Audit activities</u> including audits with the following orientation:

Risk management

- evaluate the effectiveness of, and contribute to the improvement in, risk management processes

- provide assurance that risk exposures relating to the IPC's governance, operations, and information systems are correctly evaluated, including:
  - reliability and integrity of financial and operational information
  - effectiveness, efficiency and economy of operations, and
  - safeguarding of assets
- evaluate the design, implementation, and effectiveness of the IPC's ethics-related objectives, programs, and activities
- assess whether the information technology governance sustains and supports the IPC's strategies and objectives

Compliance

- compliance with applicable laws and regulations

Performance improvement

- the efficiency, effectiveness, and economy of the IPC's business systems and processes.

(b) Advisory services

The internal audit function can advise the IPC's management on a range of matters including:

New programs, systems and processes

- providing advice on the development of new programs and processes and/or significant changes to existing programs and processes including the design of appropriate controls.

Risk management

- assisting management to identify risks and develop risk mitigation and monitoring strategies as part of the risk management framework

Fraud control

- evaluate the potential for the occurrence of fraud and how the IPC manages fraud risk
- assisting management to investigate fraud, identify the risks of fraud and develop fraud prevention and monitoring strategies.

(c) Audit support activities

The internal audit function is also responsible for:

- assisting the Audit and Risk Committee to discharge its responsibilities
- providing secretarial support to the Audit and Risk Committee
- monitoring the implementation of agreed recommendations
- disseminating across the IPC, better practice and lessons learnt arising from its audit activities.

2.1.6 Scope of internal audit activity

Internal audit reviews cover all programs and activities of the IPC, together with associated entities, as provided for in relevant business agreements, memorandum of understanding or contracts. Internal audit activity encompasses the review of all financial and non-financial policies and operations.

2.1.7 Standards

Internal audit activities will be conducted in accordance with relevant professional standards including:

- International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors
- standards issued by Standards Australia and the International Standards Organisation

- in the conduct of internal audit work, internal audit staff will:
  - comply with relevant professional standards of conduct
  - possess the knowledge, skills and technical proficiency relevant to the performance of their duties
  - be skilled in dealing with people and communicating audit, risk management and related issues effectively
  - exercise due professional care in performing their duties.

2.1.8 Relationship with external audit

Internal and external audit activities will be coordinated to help ensure the adequacy of overall audit coverage and to minimise duplication of effort.

Periodic meetings and contact between internal and external audit shall be held to discuss matters of mutual interest and facilitate coordination.

External audit will have full and free access to all internal audit plans, working papers and reports.

2.1.9 Planning

The Chief Audit Executive will prepare, for the Audit and Risk Committee's consideration, an internal audit annual audit work plan in a form agreed with the committee.

2.1.10 Reporting

The Chief Audit Executive will report to each meeting of the Audit and Risk Committee on:

- audits completed
- progress in implementing the annual audit work plan
- the implementation status of agreed internal and external audit recommendations.

The internal audit function will also report to the Audit and Risk Committee at least annually on the overall state of internal controls within IPC and any systemic issues requiring management attention based on the work of the internal audit function and other assurance providers.

2.1.11 Administrative arrangements

Any change to the position of the Chief Audit Executive or to the internal audit external service provider, will be approved by the Commissioner in consultation with the Audit and Risk Committee.

The Chief Audit Executive will arrange for an internal review, at least annually, and a periodic independent review, at least every five years, of the efficiency and effectiveness of the operations of the Internal Audit function.

2.1.12 Review of the charter

This charter shall be reviewed at least annually by the Audit and Risk Committee. Any substantive changes will be formally approved by the Commissioner on the recommendation of the Audit and Risk Committee.

2.2 Audit standards and guiding principles

Internal audit activities will be conducted in accordance with relevant professional standards. Refer Section 2.1.7 within the Internal Audit Charter above.

2.2.1 Independence and objectivity

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

Independence is the freedom from conditions that threaten the ability of the internal audit activity or the Chief Audit Executive to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the Chief Audit Executive has direct and unrestricted access to senior management and the Commissioner. Refer Section 2.1.3 above. Threats to independence must be managed at the individual auditor, engagement, functional, and organisational levels.

Objectivity is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organisational levels.

2.2.2 Organisational independence

The Chief Audit Executive must report to a level within the IPC that allows the internal audit activity to fulfil its responsibilities. The Chief Audit Executive must confirm to the Commissioner, at least annually, the organisational independence of the internal audit activity.

The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

The Chief Audit Executive must communicate and interact directly with the Commissioner.

2.2.3 Individual objectivity

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfil his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession. A conflict of interest could impair an individual's ability to perform his or her duties and responsibilities objectively.

2.2.4 Impairment to independence or objectivity

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

Impairment to organisational independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding.

The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations of the internal audit activity's and the Chief Audit Executive's responsibilities to senior management and the Commissioner as described in the internal audit charter, as well as the nature of the impairment.

Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year. Assurance engagements for functions over which the Chief Audit Executive has responsibility must be overseen by a party outside the internal audit activity.

Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.

If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

2.3 Audit and Risk Committee Charter

The Commissioner has established the Audit and Risk Committee in compliance with Treasury Circular NSW TC 09/08 August 2009.

An Audit and Risk Committee Charter, in accordance with Treasury Policy TPP 09-05 has been endorsed by the Audit and Risk Committee and approved by the Commissioner on 15 June 2011.

This charter sets out the Audit and Risk Committee's objectives, authority, composition and tenure, roles and responsibilities, reporting and administrative arrangements.

This charter is available at www.ipc.nsw.gov.au.

3 PERSONNEL

3.1 Internal audit personnel

3.1.1 Proficiency and due professional care

Internal audit engagements must be performed with proficiency and due professional care.

Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Knowledge, skills, and other competencies is a collective term that refers to the professional proficiency required of internal auditors to effectively carry out their professional responsibilities. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by the Institute of Internal Auditors and other appropriate professional organisations.

The Chief Audit Executive must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the IPC, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

An internal auditor must decline a consulting engagement or obtain competent advice and assistance if he or she lacks the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Due professional care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

Internal auditors must exercise due professional care by considering the:

- extent of work needed to achieve the engagement's objectives;
- relative complexity, materiality, or significance of matters to which assurance procedures are applied;
- adequacy and effectiveness of governance, risk management, and control processes;

- probability of significant errors, fraud, or non-compliance; and
- cost of assurance in relation to potential benefits.

In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

Internal auditors must exercise due professional care during a consulting engagement by considering the:

- needs and expectations of clients, including the nature, timing, and communication of engagement results;
- relative complexity and extent of work needed to achieve the engagement's objectives; and
- cost of the consulting engagement in relation to potential benefits.

Continuing professional development

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

4 AUDIT PLANNING

4.1 Planning

Audit planning is essential in order to ensure that the internal audit effort is directed to areas that will provide the most benefit and add the most value to the IPC.

Planning indicates future intended actions. While all attempts should be made to achieve plans, it should be recognised that planning is a dynamic process that occurs continually throughout any process and any plans should be adjusted as required where new circumstances or new insights indicate such adjustment is warranted.

4.1.1 Strategic audit planning

The Chief Audit Executive must, in consultation with the internal audit service providers and the Audit and Risk Committee establish long-term, strategic, risk-based plans to determine the priorities of the internal audit activity, consistent with the IPC's goals.

The Chief Audit Executive is responsible for providing to the Audit and Risk Committee a three-year strategic audit plan, which is based on the IPC's current understanding of its risks. The IPC's risk management framework should be considered in performance of this task, including considering the risk appetite levels set by management for the different activities or parts of the organisation. Where a risk has been identified that has not yet been included in the risk management framework, the Chief Audit Executive should exercise his/her own judgment of risks after consultation with the Internal Audit service providers, senior management and the Commissioner.

This strategic audit plan is indicative only and generally not costed. Its purpose is to ensure that there is reasonable internal audit coverage of all relevant risk areas and key internal control systems over time.

The strategic audit plan should be provided to the Audit and Risk Committee each year for discussion and endorsement prior to the approval of the annual audit plan.

4.1.2 Annual audit plan

The annual audit plan of engagements must be based on a documented risk assessment and undertaken at least annually. The input of the internal audit service provider, senior management and the Commissioner must be considered in this process.

The Chief Audit Executive should consider accepting proposed consulting engagements, either from the outsourced internal audit service provider or another appropriately experienced third party, based on the engagement's potential to improve management of risks, add value, and improve the IPC's operations. Accepted engagements must be included in the plan. The plan should be fully costed.

4.1.3 Field audit plan

The internal audit service provider will plan the engagement such that the work is performed in the most efficient and effective manner and that all reasonable attempts are made to achieve the engagement objectives to appropriate professional standards and within the agreed time budget for the engagement.

The objectives, scope, timing, fees and key contacts for each review should be formally agreed with the Chief Audit Executive and documented prior to commencement.

Detailed plans of audit procedures should be formally documented but are not generally provided to the Chief Audit Executive as a matter of course, although they remain the property of the IPC and should be made available on request.

Responsibility for the efficient and effective execution of individual engagements rests with the internal audit service provider under the oversight of the Chief Audit Executive. Common considerations in engagement planning are detailed further at heading 4.3 below.

4.1.4 Communication and approval

The Chief Audit Executive must communicate the strategic audit plan, the annual audit plan and associated resource requirements to the Audit and Risk Committee each year for endorsement and the Commissioner for final review and approval. The Chief Audit Executive must also communicate to the Audit and Risk Committee and the Commissioner the impact that any resource limitations is projected to have on the effectiveness of internal audit.

4.1.5 Resource management

The Chief Audit Executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimises the achievement of the approved plan.

The time usage of third party service providers is accountable through the contract management procedures in place within the IPC, whereby the scope for each assurance and consulting engagement are agreed with the Chief Audit Executive prior to the commencement of the engagement. Variations to the scope of any project must be negotiated with the Chief Audit Executive as soon as is practicable and before the scope of the project are exceeded.

The Chief Audit Executive may authorise or refuse any variation at his or her discretion.

4.1.6 Coordination

The Chief Audit Executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimise duplication of efforts.

4.1.7 Reporting to senior management and the Commissioner

The Chief Audit Executive must report periodically to senior management and the Commissioner via the Audit and Risk Committee on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the Commissioner.

The frequency and content of reporting are determined in discussion with senior management and the Commissioner and depend on the importance of the information to be communicated and the urgency of the related actions to be taken.

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

4.2 Nature of work

4.2.1 Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the IPC
- Ensuring effective organisational performance management and accountability
- Communicating risk and control information to appropriate areas of the IPC
- Coordinating the activities of and communicating information among the Commissioner, external and internal auditors, and management.

The internal audit activity must evaluate the design, implementation, and effectiveness of the IPC's ethics-related objectives, programs, and activities.

The internal audit activity must assess whether the information technology governance of IPC sustains and supports its strategies and objectives.

Consulting engagement objectives must be consistent with the overall values and goals of the IPC.

4.2.2 Risk management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- the IPC's objectives support and align with its mission
- significant risks are identified and assessed
- appropriate risk responses are selected that align risks with the IPC's risk appetite
- relevant risk information is captured and communicated in a timely manner across IPC, enabling staff, management, and the Commissioner to carry out their responsibilities
- risk management processes are monitored through ongoing management activities, separate evaluations, or both.

The internal audit activity must evaluate risk exposures relating to the IPC's governance, operations, and information systems regarding the:

- reliability and integrity of financial and operational information
- effectiveness and efficiency of operations
- safeguarding of assets
- compliance with laws, regulations, and contracts.

The internal audit activity must evaluate the potential for the occurrence of fraud and how the IPC manages fraud risk.

During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the IPC's risk management processes.

When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

4.2.3 Control processes

The internal audit activity must assist the IPC in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within its governance, operations, and information systems regarding the:

- reliability and integrity of financial and operational information
- effectiveness and efficiency of operations
- safeguarding of assets
- compliance with laws, regulations, and contracts.

4.3 Engagement planning

Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the IPC.

Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.

During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.

Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the IPC's control processes.

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

4.3.1 Planning considerations

In planning the engagement, internal auditors must consider:

- the objectives of the activity being reviewed and the means by which the activity controls its performance
- the significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level
- the adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model
- the opportunities for making significant improvements to the activity's risk management and control processes.

When planning an engagement for parties outside the IPC (for example, audits of third party service providers, or partner agencies, etc), internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

4.3.2 Engagement objectives

Objectives must be established for each engagement. Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

Internal auditors must consider the probability of significant errors, fraud, non-compliance, and other exposures when developing the engagement objectives.

Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria.

Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.

4.3.3 Engagement scope

The established scope must be sufficient to satisfy the objectives of the engagement.

The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

4.3.4 Engagement resource allocation

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

4.3.5 Engagement work program

Internal auditors must develop and document work programs that achieve the engagement objectives.

Work programs must include the procedures for identifying, analysing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.

Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

5 AUDIT METHODOLOGY

5.1 The audit cycle – summary

The audit process features four phases:

- engagement planning
- fieldwork
- reporting audit results and audit closure
- audit monitoring.

Audit engagement planning

The engagement planning phase involves selecting and providing resources for the audit, notifying the audited entity, conducting the entry conference, collecting preliminary information, defining the audit objectives, scope and methodology, and preparing an audit plan and program. This is addressed at Section 4.3 above.

Audit fieldwork

Audit fieldwork involves executing the audit plan and audit program in accordance with IIA Standards and this manual. All working papers should be recorded electronically, where practicable. Activities central to the fieldwork phase include: collecting and analysing information, developing findings, conclusions and recommendations, discussing issues with appropriate IPC personnel, and documenting evidence. The fieldwork phase ends with the holding of the exit meeting.

Reporting audit results and audit closure

During the reporting phase, the internal auditor formally communicates audit results, conclusions and recommendations to relevant IPC personnel. The audit team prepares the draft and final audit report for management's review and issuance to the IPC.

Audit monitoring

The audit monitoring phase involves following-up with the audited body's management on the status of implementation of audit recommendations and resolving long-outstanding recommendations.

5.2 Risk and control analysis

5.2.1 Risk assessment

Risk assessment is conducted at the activity-level to identify and evaluate risk exposures at the operations or divisional level of the IPC. It involves considering business process risks, quality of local management and individual performance in different situations. As part of the planning activities, the risks that threaten the objectives of each process or sub-focus area within the activity to be audited should be identified and classified into the respective risk categories. The purpose of the risk assessment at the activity-level is to determine the audit objectives.

The audit will concentrate on those sub-focus areas that are assessed as moderate or higher risk. The risk categories of the sub-focus areas indicate the types of objectives that should be included in the audit program.

For example where compliance risks are rated as moderate or high, the auditor should ensure that the audit objectives include a review of compliance with the procedures/policies related to the activity. If operational risks are higher, the objectives should include a review of the efficiency and effectiveness of the procedures and policies.

The focus area may also be a determinant of the type of audit to be conducted. For example, the focus area of Program and Project Management or Strategy Management and Governance may indicate the need for a performance audit; an IT Management focus area may indicate the need for an IT audit etc.

5.2.2 Control analysis

All audits, regardless of the nature, typically involve providing assurance on the design and effectiveness of the system of internal control. After obtaining an understanding of the internal control system by way of interviews, questionnaires, systems documentations, walk-throughs and/or performing some initial analytical procedures or data analysis, auditors should make a preliminary assessment of the internal control system to determine whether identified controls are designed to meet the control objectives and mitigate risks. Examination of documents, records and reports should be undertaken to assess the design of the controls.

5.2.3 Analysis and evaluation

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations, including the collection of audit evidence.

Audit evidence refers to all the information used by the auditor in arriving at the audit opinions, conclusions and recommendations. It is obtained through applying audit procedures such as observing conditions, interviewing people, examining records and analysing data. In forming the audit opinion, the auditor need not review all the information available because conclusions can sometimes be reached by using sampling approaches and other means of selecting items for examination. Audit evidence is cumulative in nature and is persuasive rather than conclusive. Audit inferences are drawn from the body of evidence collected.

Audit evidence should be sufficient, competent, relevant and useful:

- Sufficient information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor. There should be enough of it to support the auditor's findings. In determining the sufficiency of evidence it may be helpful to ask such questions as: Is there enough evidence to persuade a reasonable person of the validity of the findings? When should appropriate statistical sampling methods be used to establish sufficiency?
- Competent information is reliable and the best attainable through the use of appropriate engagement techniques, such as statistical sampling and analytical audit procedures. Information is more competent if it is (i) obtained from an independent source, (ii) corroborated by other information, (iii) obtained directly by the auditor, such as through personal observation, (iv) documented, and (v) an original document rather than a copy.
- Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement. Relevant information should have a logical, sensible relationship with the associated audit finding.
- Useful information helps the IPC meets its goals.

Evidence collected by auditors should possess all of these qualities. For example, it is not enough to merely interview staff members without corroborating the information obtained with that from other sources. Sample sizes should be representative so that conclusions reached may be validly extended to the rest of the population.

Evidence may be categorised as physical, documentary, testimonial and analytical and is obtained by using various procedures:

Physical evidence

Physical evidence is obtained by direct inspection or observation of people, property or events. Inspection of tangible assets provides reliable audit evidence about their existence, but not necessarily as to their ownership or value. Observation consists of looking at a process or procedure being performed by others, for example, physically counting inventory and making observations. The observations of certain procedures are important particularly those that do not leave an audit trail.

Documentary evidence

Documentary evidence consists of information that exists in some permanent form such as letters, contracts, accounting records, invoices, and management information on performance. It is the most common form of evidence; it may be internal, external or a combination of both. The source of documentary evidence affects its reliability.

Testimonial evidence

Testimonial evidence is obtained through inquiries, interviews, or questionnaires. Inquiry and confirmation consists of seeking information from knowledgeable persons inside or outside the IPC. Responses to inquiries may provide auditors with information not previously possessed or with corroborative audit evidence. Testimonial evidence may not always be conclusive and should be supported by other forms of information where possible.

Analytical evidence

Analytical evidence arises from the application of analytical procedures. Analytical procedures produce information in the form inferences or conclusions based on examining data for consistencies, inconsistencies, cause-effect relationships etc.

Audit criteria

The auditor should clarify the specific explicit or implicit criteria against which evidence collected will be evaluated. Criteria are explicit when they are clearly set out in policies, manuals, standard operating procedures, standards, laws and/or regulations. Where management has not yet established goals and objectives or determined the controls needed in a particular area, it may be necessary to develop implicit criteria based on what management considers being satisfactory performance standards or industry best practices. The acceptability of implicit criteria should always be confirmed with the audited entity. Conducting an audit without agreeing the criteria may result in conclusions and recommendations that may not be accepted by the audited entity and lead to wasted audit effort and fruitless arguments.

Analysis of financial data

During fieldwork, analytical procedures should be used to support the results of the assignment. Auditors should consider the factors listed below in determining the extent to which analytical audit procedures should be used. After evaluating these factors, internal auditors should consider the use of additional audit procedures, as necessary, to achieve the engagement objectives:

- the significance of the area being examined
- the assessment of risk and effectiveness of risk management in the area being examined;
- The adequacy of the system of internal control
- the availability and reliability of financial and non-financial information
- the precision with which the results of analytical audit procedures can be predicted
- the availability and comparability of information regarding the industry in which the IPC operates, including other NSW government agencies
- the extent to which other engagement procedures provide support for engagement results.

When analytical audit procedures identify unexpected results or relationships, internal auditors should examine and evaluate such results or relationships. This examination and evaluation should include making inquiries of management, and applying other engagement procedures until internal auditors are satisfied that the results or relationships are sufficiently explained. Unexplained results or relationships from applying analytical audit procedures may be indicative of a significant condition such as a potential error, irregularity, or illegal act. Results or relationships that are not sufficiently explained should be communicated to the appropriate levels of management. Internal auditors may recommend appropriate courses of action, depending on the circumstances.

Analysis of other data and processes

The principles applied in analysing financial data can also be utilised in examining other data, activities and processes. Directives, policies, contracts etc. may be analysed to determine their significant elements, and these assessed against best practices, standards or benchmarks. The work of committees/teams/working groups may be analysed to determine their mandate, functions, areas of responsibility, reporting lines, frequency of meetings and how decisions are implemented. By breaking activities into their composite elements, auditors may conduct analyses by observing trends, making comparisons and isolating unusual transactions and conditions for follow-up.

Detailed audit procedures

In addition to analytical procedures and techniques, auditors may perform the following detailed audit tests during the fieldwork:

- Vouching – testing recorded amounts by examining supporting documents to determine whether they represent an actual transaction.
- Tracing – following a document through its processing cycles to the accounting records to determine whether all transactions have been recorded
- Re-computation – verifying the mathematical accuracy of figures. The value of this procedure is limited as the reliability of the evidence obtained depends on the validity of the underlying input.
- Scanning – searching for obvious exceptions in a large quantity of data.

Evaluation

Evaluation is a means of arriving at a professional judgment. As auditors compare circumstances observed against relevant criteria, they evaluate the significance of any variance and determine whether corrective action is necessary. The analysis and evaluation of evidence obtained should give rise to issues (positive and negative), which internal audit may report to management.

Auditors should draw conclusions for each audit objective. Conclusions are logical inferences about the audit subject based on the auditors' findings. Conclusions should be specified and not left to be inferred by readers. The strength of a conclusion depends on the persuasiveness of the evidence supporting the findings, and how convincing the logic used to formulate the conclusions is. They should be free from personal biases or prejudices, and be objective. The conclusion reached by internal audit should be the same as would have been reached by a similar experienced professional reviewing the same evidence.

5.3 Audit programs

Audit programs, i.e. the plan of work for the conduct of an individual engagement to conduct the risk and control analysis, including the collection and assessment of audit evidence, are created by the internal audit service provider during the performance of the audit using research and past experience as a guide.

Audit programs should be included in the audit working papers, which are retained by the internal audit service provider on behalf of the IPC, which retains ownership of the working papers.

5.4 Working papers

Internal auditors must create working papers for each engagement. Such working papers must document relevant information to support the conclusions and engagement results.

Working papers remain the property of IPC, but will generally be retained by the internal audit service provider, who will provide them to the Chief Audit Executive promptly upon request.

The Chief Audit Executive must control access to engagement records. The Chief Audit Executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

The Chief Audit Executive must apply NSW State Records retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the IPC Records Management Policy.

The Chief Audit Executive must apply due diligence in governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with IPC's guidelines and any pertinent regulatory or other requirements.

5.4.1 Recording information during the audit

Auditors should record all elements of the assignment as working papers in audit files. Audit files should document the planning process, the evaluation of the adequacy and effectiveness of the relevant segments of the internal control system, each audit step performed, the information obtained and the conclusions reached. The contents of the file should clearly support the bases of the observations and recommendations to be reported to the audited entity, and provide evidence that the audit was performed in accordance with IIA Standards.

Working papers should be developed in a timely manner as the audit progresses. They help to enhance the quality of the audit and facilitate effective review and evaluation of the audit evidence obtained and conclusions reached before the audit report is finalised.

The file should be detailed enough to enable an experienced auditor, having no previous connection with the audit, to understand the (i) nature, timing, and extent of the audit procedures performed; (ii) results of the procedures and the audit evidence obtained; and (iii) significant matters arising during the audit and the conclusions reached. The working papers should also explain why any audit program step was not executed.

Each working paper should:

- identify the assignment and describe the contents or purpose of the working paper
- bear the initials of the auditor performing the work and the date prepared
- contain an index or reference number and cross-referenced to related working papers as appropriate
- explain any tick marks used
- clearly identify the source(s) of data.

Audit files should also include the following:

- the specific audit objective
- a description of the related risks identified
- a description of the population tested (including the size)
- the size of the sample tested and the sampling methodology used
- conclusions reached.

5.5 Reporting audit results

5.5.1 Communicating results

Internal auditors must communicate the engagement results. Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

Final communication of engagement results must, where appropriate, contain internal auditors' overall opinion and/or conclusions.

Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

When releasing engagement results to parties outside the IPC, the communication must include limitations on distribution and use of the results.

Quality of communications

Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair minded and balanced assessment of all relevant facts and circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the IPC and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

Errors and omissions

If a final communication contains a significant error or omission, the Chief Audit Executive must communicate corrected information to all parties who received the original communication.

5.5.2 Disseminating results

The Chief Audit Executive must communicate results to the appropriate parties.

The Chief Audit Executive or designee reviews and approves the final engagement communication before issuance and decides to whom and how it will be disseminated.

The Chief Audit Executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside IPC the Chief Audit Executive must:

- assess the potential risk to the IPC
- consult with senior management and/or legal counsel as appropriate
- control dissemination by restricting the use of the results.

The Chief Audit Executive is responsible for communicating the final results of consulting engagements.

During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the IPC, they must be communicated to senior management and the Commissioner.

5.5.3 Audit findings

Auditors should report audit findings i.e. significant deviations from relevant criteria, to management so that corrective action can be taken. A reportable finding is a significant condition which:

- warrants the attention of management
- is documented by facts, not opinions, and by evidence that is sufficient, competent and relevant
- is objectively developed without bias or preconceived ideas
- is relevant to the issue involved
- is convincing enough to compel action to correct the defective condition.

Audit findings should contain the elements of criteria, condition, cause effect and recommendation.

- **Criteria**
  The standards, measures, or expectations used in making an evaluation and/or verification (what should exist). The criteria should be credible, convincing and objective. They should be designed to meet a management goal.
- **Condition**
  The factual evidence that the internal auditor found in the course of the examination (what does exist). The condition should include sufficient information to promote an adequate understanding of the matter(s) being reported.
- **Cause**
  The reason for the difference between the expected and actual conditions. i.e. why the difference exists. The cause should be complete and go to the heart of the problem; not just the symptom.
- **Effect**
  The risk or exposure to the IPC and/or others encountered because the condition is not consistent with the criteria (the impact of the difference). The effect should be logical and likely to occur.
- **Recommendations**
  Recommendations are based on the internal auditor's observations and conclusions. They call for action to correct existing conditions or improve operations. Recommendations may suggest general or specific approaches to correcting or enhancing performance as a guide for management in achieving desired results. They should address the cause of the finding, be implementable and capable of being monitored.

Formulating recommendations

The main objective of an audit is to provide assurance as to the efficiency and effectiveness of established internal controls, to develop recommendations for improving them, and to ensure compliance with the IPC's rules and policies. Recommendations should be made when there is a potential to improve performance, to enhance policies and procedures, to mitigate risks identified, and in cases when significant instances of non-compliance or weaknesses in internal controls were noted.

Recommendations should be constructive, practical, action oriented and thoroughly discussed with the audited entity as to their feasibility and practicality. All audit recommendations should be specific, stand alone, and must address the cause of the deficiency. Unless the recommendation addresses the cause of a deficiency, the probability of the deficiency being corrected is considerably reduced.

Generally, audit recommendations are most effective and acceptable to the audited entity when they are:

- constructive and directed at improved or enhanced performance
- directed at correcting the cause of the problem identified
- action-oriented in that they suggest specific steps that should be taken to change, modify, or otherwise perform some action
- addressed to officials that are empowered to act
- feasible, achievable, practical, cost effective
- aiming to recover or save resources.

Record of control weaknesses

The actual or potential effect of every finding should be determined and quantified, if possible. The auditor should determine the possible financial implications of outcomes such as:

- cost savings, making scarce human financial and operational resources available for other program/mission-related use
- cost avoidance by reducing expenditures and making funds available for other essential purposes
- recovery of any amounts overpaid or incorrectly paid
- possibilities for income generation.

In developing the audit finding, the auditor should explain the assumptions made in determining the expected financial implications. The amount of the saving or recovery should be stated in the text of the audit recommendation, whenever possible. If an exact figure cannot be determined, a reasonable, conservative estimate should be made. Where the financial implication arises from the examination of a sample, the recommendation should request the audited entity to conduct a further examination of the population to determine the full extent of the saving or recovery, and to take action to save or recover the amount already established as a minimum. The detailed assumptions and calculations need to be documented in the audit file.

Auditors should consider the degree/impact of the deficient condition before deciding to communicate it formally to management. Including insignificant deviations (clerical errors, one-off inconsistencies, etc.) alongside considerable actual or potential losses or risks serves to devalue more important matters on which management should focus. Instead, the auditor should discuss insignificant issues with the activity owner and check that the situation is corrected. The matter should be noted in the working papers. Minor issues that have been satisfactorily resolved need not be mentioned in detail in the audit report except to indicate that the issues were discussed with the IPC's representatives and were satisfactorily resolved. More significant issues, even if they have been resolved should be reported in the Audit Report.

Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff are developed.

The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The internal audit service provider has overall responsibility for supervising the engagement. Appropriate evidence of supervision is documented and retained in the working papers.

5.6 Audit sampling

Audit sampling involves the application of audit procedures to less than 100 per cent of the population such that each item in the population has an equal chance of being selected. Sampling enables auditors to obtain and evaluate audit evidence about some characteristic of the items selected (sample) in order to form or assist in forming a conclusion about the population from which the sample is drawn.

Audit sampling can use either a statistical or a non-statistical approach. Statistical sampling means any approach to sampling that has the following characteristics:

- random selection of a sample
- use of probability theory to evaluate sample results, including measurement of sampling risk. Sampling risk arises from the possibility that the auditor's conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure.

Any sampling approach that does not fulfil the characteristics set out above for statistical sampling is considered non-statistical sampling. The results of testing a sample using a non-statistical sampling approach should not be extrapolated over the population as the sample is unlikely to be representative of the population.

5.6.1 Choice of sampling method and technique

The sampling method selected depends on the audit objective. If the auditor is seeking to determine how many cases or how much (the amount) of something exists, s/he should use a statistical sampling method. If on the other hand, the auditor wants to determine whether a problem exists, s/he should use non-statistical sampling.

There are two types of statistical sampling – attributes sampling and variables sampling.

Attribute sampling

Attribute sampling provides answer to the question “How many items display the characteristic or attribute I am seeking to identify?” It allows the auditor to determine whether the rate of occurrence of a characteristic or attribute (usually errors) in a population is small enough to assume that procedures are working effectively or is indicative of an issue that needs to be included in the audit report. It is applied to testing items that can have only two possible values (e.g., 0 or 1) or attributes (e.g., correct or incorrect, or yes or no).

Attribute sampling is most widely used in tests of control (to determine rates of non-compliance within control procedures). Attribute sampling selection techniques include survey sampling and decision sampling.

Variables sampling

Variables sampling provides answer to the question “How much”? It is usually applied to stated monetary amounts and attempts to provide information about their accuracy. By taking a sample and drawing an inference about the population, the auditor can reach a conclusion on whether the amount is materially misstated. Variables sampling is used in substantive tests of details.

Variables sampling selection techniques include simple and systematic random sampling and stratified sampling.

Non-statistical sampling is based on the auditor’s judgement. It is appropriate when looking for the existence of a problem or when the auditor does not need to draw conclusions about the entire population. Non-statistical sampling selection techniques include haphazard, judgement, convenience and biased sampling.

The decision whether to use a statistical or non-statistical sampling approach is a matter for the auditor’s professional judgement regarding the most efficient manner to obtain appropriate audit evidence in the particular circumstances. To the extent possible, statistical sampling should be used in all audits.

5.6.2 Testing the whole population

Sampling is not always required and it may be possible to apply audit procedures to the entire population if all the data is held on computer systems and data analysis software is available. The auditor may also decide not to sample if:

- the population is small
- she/he is unwilling to accept the sampling risk
- she/he is searching for rare occurrences or known problem areas.

5.7 Audit monitoring

The Chief Audit Executive must establish and maintain a system to monitor the disposition of results communicated to management.

The Chief Audit Executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

A status of all audit recommendations should be reported to the Audit and Risk Committee.

Internal audit has the responsibility to follow up and determine whether or not the IPC has taken steps to adequately, effectively and timely address the matters reported in audit findings and recommendations. The ultimate success of the audit occurs when the IPC takes appropriate steps to reduce risks or improve operations as recommended by the audit.

Internal audit therefore should monitor the status of implementation of open recommendations until the reported issue is either solved or the appropriate level of management has accepted the risk.

An extract of all open recommendations should be produced and made available to the Audit and Risk Committee including:

- date of recommendation
- recommendation number
- recommendation status
- text of the recommendation
- risk category and rating
- history of the audited entity's comments
- estimated target date for implementation of the recommendation
- a column for the audited entity's updated comments.

5.7.1 Resolution of senior management's acceptance of risks

When the Chief Audit Executive believes that IPC management has accepted a level of residual risk that may be unacceptable to the IPC, the Chief Audit Executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the Chief Audit Executive must report the matter to the Commissioner for resolution, generally via the Audit and Risk Committee.

The primary function of internal audit is to assist IPC to accomplish its objectives by evaluating its risk management, control and governance processes, and making recommendations to mitigate risks or improve effectiveness. The Executive Director is responsible for deciding the appropriate action to be taken in response to reported audit findings and recommendations. Managers are responsible for assessing the actions taken by management and determining whether matters reported as audit findings and recommendations were resolved in a timely manner. Where IPC management decides to assume the risk of not correcting the reported condition because of cost or other considerations, the implication of their decision should be brought to their attention formally.

The Chief Audit Executive should assess the risk to the IPC of all recommendations that have remained open for a significant period of time. The Chief Audit Executive should bear in mind that some recommendations may necessarily require more time for full implementation and allow reasonable time for such recommendations.

The Chief Audit Executive should liaise with the internal audit service provider and agree the assessment of open recommendations, where practicable.

6 ONGOING AUDIT ENGAGEMENTS AND DEVELOPMENT AUDITS

As described in section 5.3 above, Audit Programs, containing the Audit Objectives and Audit Approach are prepared for each engagement and these are retained with the audit working papers. It is neither necessary nor efficient to update the manual with each change in each program every time an audit is conducted, as is implied by these headings.

For recurring audit engagements, the previous objectives, approach and working papers will be examined for ongoing relevance as part of the planning process for the audit.

For new audit engagements, appropriate objectives and audit approach will be determined through the normal audit planning consultations in section 4.

7 ENGAGEMENT EVALUATIONS & PERFORMANCE REVIEWS

7.1 Quality assurance and improvement program

The Chief Audit Executive must ensure that there is in place a quality assurance and improvement program that covers all aspects of the internal audit activity.

A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the IIA's Definition of Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

The quality assurance and improvement program must include both internal and external assessments, generally performed on the internal audit service provider.

7.1.1 Internal assessments

Internal assessments must include:

- ongoing monitoring of the performance of the internal audit activity; and
- periodic reviews performed through self-assessment or by other persons within the IPC with sufficient knowledge of internal audit practices.

Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the IIA's Definition of Internal Auditing, the Code of Ethics, and the Standards.

Periodic reviews are assessments conducted to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.

Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

7.1.2 External assessments

External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the IPC. The Chief Audit Executive must discuss with the Commissioner:

- the need for more frequent external assessments
- the qualifications and independence of the external reviewer or review team, including any potential conflict of interest.

A qualified reviewer or review team consists of individuals who are competent in the professional practice of internal auditing and the external assessment process. The evaluation of the competency of the reviewer and review team is a judgment that considers the professional internal audit experience and professional credentials of the individuals selected to perform the review. The evaluation of qualifications also considers the size and complexity of the agencies that the reviewers have been associated with, in relation to the IPC, for which the internal audit activity is being assessed, as well as the need for particular sector, industry, or technical knowledge.

An independent reviewer or review team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the IPC or the outsourced service provider.

7.1.3 Reporting on the quality assurance and improvement program

The Chief Audit Executive must communicate the results of the quality assurance and improvement program to senior management and the Commissioner.

The form, content, and frequency of communicating the results of the quality assurance and improvement program is established through discussions with senior management and the Commissioner and considers the responsibilities of the internal audit activity and Chief Audit Executive as contained in the internal audit charter. To demonstrate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards, the results of external and periodic internal assessments are communicated upon completion of such assessments and the results of ongoing monitoring are communicated at least annually. The results include the reviewer's or review team's assessment with respect to the degree of conformance.

(a) Use of "conforms" with the International Standards for the Professional Practice of Internal Auditing

The Chief Audit Executive may state that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing only if the results of the quality assurance and improvement program support this statement.

(b) Disclosure of non-conformance

When non-conformance with the Definition of Internal Auditing, the Code of Ethics, or the Standards impacts the overall scope or operation of the internal audit activity, the Chief Audit Executive must disclose the non-conformance and the impact to senior management and the Commissioner.

GLOSSARY

Add value

Value is provided by improving opportunities to achieve the agency's organisational objectives, identifying operational improvement, and/or reducing risk exposure through both assurance and consulting services.

Adequate control

Present if management has planned and organised (designed) in a manner that provides reasonable assurance that the agency's risks have been managed effectively and that its goals and objectives will be achieved efficiently and economically.

Assurance services

An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the agency. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Board

A board is an organisation's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors, or any other designated body of the organisation, including the audit committee to whom the Chief Audit Executive may functionally report.

Charter

The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the agency; authorises access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

Chief Audit Executive

Chief Audit executive is a senior position within the agency responsible for internal audit activities. Normally, this would be the internal audit director. In the case where internal audit activities are obtained from external service providers, the Chief Audit Executive is the person responsible for overseeing the service contract and the overall quality assurance of these activities, reporting to senior management and the Commissioner regarding internal audit activities, and follow-up of engagement results. The term also includes titles such as general auditor, head of internal audit, chief internal auditor, and inspector general.

Code of Ethics

The Code of Ethics of the Institute of Internal Auditors (IIA) are principles relevant to the profession and practice of internal auditing, and Rules of Conduct that describe behaviour expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.

Compliance

Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

Conflict of interest

Any relationship that is, or appears to be, not in the best interest of the agency. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

Consulting services

Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an agency's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Control

Any action taken by management, the Commissioner, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organises, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Control environment

The attitude and actions of the Commissioner and management regarding the significance of control within the agency. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values
- Management's philosophy and operating style
- Organisational structure
- Assignment of authority and responsibility
- Human resource policies and practices
- Competence of personnel.

Control processes

The policies, procedures, and activities that are part of a control framework, designed to ensure that risks are contained within the risk tolerances established by the risk management process.

Engagement

A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

Engagement objectives

Broad statements developed by internal auditors that define intended engagement accomplishments.

Engagement work program

A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.

External service provider

A person or firm outside of the agency that has special knowledge, skill, and experience in a particular discipline.

Fraud

Any illegal act characterised by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organisations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

Governance

The combination of processes and structures implemented by the Commissioner to inform, direct, manage, and monitor the activities of the agency toward the achievement of its objectives.

Impairment

Impairment to organisational independence and individual objectivity may include personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).

Independence

The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional, and organisational levels.

Information technology controls

Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.

Information technology governance

Consists of the leadership, organisational structures, and processes that ensure that the agency's information technology sustains and supports the agency's strategies and objectives.

Internal audit activity

A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve the agency's operations. The internal audit activity helps the agency accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

International professional practices framework

The conceptual framework that organises the authoritative guidance promulgated by the IIA. Authoritative guidance is comprised of two categories – (1) mandatory and (2) strongly recommended.

Must

The Standards use the word "must" to specify an unconditional requirement.

Objectivity

An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Objectivity requires internal auditors not to subordinate their judgment on audit matters to others.

Residual risk

The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.

Risk

The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Risk appetite

The level of risk that the agency is willing to accept.

Risk management

A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the agency's objectives.

Should

The Standards use the word "should" where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

Significance

The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

Standard

A professional pronouncement promulgated by the Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance.

Technology-based audit techniques

Any automated audit tool, such as generalised audit software, test data generators, computerised audit programs, specialised audit utilities, and computer-assisted audit techniques (CAATs).

ATTACHMENT 1

Internal Audit Charter

PREFACE

We aim to be an effective organisation. Having appropriate governance structures including sound risk management and internal audit processes is one way of achieving this.

PURPOSE

Internal audits are an integral part of the corporate governance framework of the Information and Privacy Commission (IPC). This charter provides the framework for the conduct of the internal audit function in our office.

PURPOSE OF INTERNAL AUDIT

Internal audit 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.

Internal audit provides an independent and objective review and advisory service to:

- provide assurance to the Information Commissioner, the IPC executive team and the Audit and Risk Committee, that the IPC's financial and operational controls, designed to manage the organisation's risks and achieve the entity's objectives, are operating in an efficient, effective and ethical manner
- assist management in improving the entity's business performance.

INDEPENDENCE

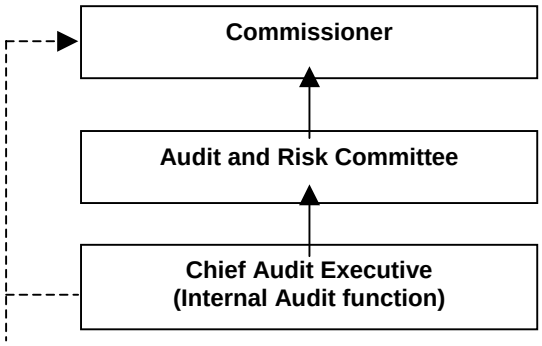
Independence is essential to the effectiveness of the internal audit function. Internal audit activity must be independent, and internal auditors must be objective in performing their work. Internal auditors must have an impartial, unbiased attitude and avoid any conflicts of interest.

The internal audit function has no direct authority or responsibility for the activities it reviews. The internal audit function has no responsibility for developing or implementing procedures or systems and does not prepare records or engage in original line processing functions or activities.

The internal audit function is responsible on a day-to-day basis to the Chief Audit Executive.

The internal audit function, through the Chief Audit Executive, reports functionally to the Audit and Risk Committee on the results of completed audits and for strategic direction and accountability purposes, and reports administratively to the Commissioner to facilitate day-to-day operations.

The following reporting line is prescribed:



AUTHORITY AND CONFIDENTIALITY

Internal auditors are authorised to have full, free and unrestricted access to all functions, premises, assets, personnel, records, and other documentation and information that the Chief Audit Executive considers necessary to enable the internal audit function to meet its responsibilities.

All records, documentation and information accessed in the course of undertaking internal audit activities are to be used solely for the conduct of these activities. The Chief Audit Executive and individual internal audit staff are responsible and accountable for maintaining the confidentiality of the information they receive during the course of their work.

All internal audit documentation is to remain the property of the IPC, including where internal audit services are performed by an external third party provider.

ROLES AND RESPONSIBILITIES

The internal audit function must evaluate and contribute to the improvement of governance, risk management and control processes using a systematic and disciplined approach.

In the conduct of its activities, the internal audit function will play an active role in:

- developing and maintaining a culture of accountability and integrity
- facilitating the integration of risk management into day-to-day business activities and processes
- promoting a culture of cost-consciousness, self-assessment and adherence to high ethical standards.

Internal audit activities will encompass the following areas:

1. Risk management

- evaluate the effectiveness of, and contribute to the improvement in risk management processes
- provide assurance that risk exposures relating to the organisation's governance, operations, and information systems are correctly evaluated, including:
    - reliability and integrity of financial and operational information
    - effectiveness, efficiency and economy of operations, and
    - safeguarding of assets
- evaluate the design, implementation and effectiveness of the organisation's ethics-related objectives, programs, and activities
- assess whether the information technology governance of the organisation sustains and supports the organisation's strategies and objectives.

2. Compliance

- evaluate compliance with applicable laws and regulations

3. Performance improvement

- evaluate the efficiency, effectiveness, and economy of the entity's business systems and processes.

ADVISORY SERVICES

The internal audit function can advise the IPC Executive Team on a range of matters including:

1. New programs, systems and processes

- providing advice on the development of new programs and processes and/or significant changes to existing programs and processes including the design of appropriate controls

2. Risk management

- assisting management to identify risks and develop risk mitigation and monitoring strategies as part of the risk management framework

3. Fraud control

- evaluate the potential for the occurrence of fraud and how the IPC manages fraud risk
- assisting management to investigate fraud, identify the risks of fraud and develop fraud prevention and monitoring strategies.

AUDIT SUPPORT ACTIVITIES

The internal audit function is also responsible for:

- assisting the Audit and Risk Committee to discharge its responsibilities
- providing secretarial support to the Audit and Risk Committee
- monitoring the implementation of agreed recommendations
- disseminating across the entity better practice and lessons learnt arising from its audit activities.

SCOPE OF INTERNAL AUDIT ACTIVITIES

Internal audit reviews cover all programs and activities of the IPC together with associated entities, as provided for in relevant business agreements, memoranda of understanding or contracts. Internal audit activity encompasses the review of all financial and non-financial policies and operations.

STANDARDS

Internal audit activities will be conducted in accordance with relevant professional standards including:

- International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors
- standards issued by Standards Australia and the International Standards Organisation.

In the conduct of internal audit work, internal audit staff will:

- comply with relevant professional standards of conduct
- possess the knowledge, skills and technical proficiency relevant to the performance of their duties
- be skilled in dealing with people and communicating audit, risk management and related issues effectively
- exercise due professional care in performing their duties.

RELATIONSHIP WITH EXTERNAL AUDIT

Internal and external audit activities will be coordinated to help ensure the adequacy of overall audit coverage and to minimise duplication of effort.

Periodic meetings and contact between internal and external audit shall be held to discuss matters of mutual interest and facilitate coordination.

External audit will have full and free access to all internal audit plans, working papers and reports.

PLANNING

The Chief Audit Executive will prepare, for the Audit and Risk Committee's consideration, an internal audit annual audit work plan in a form agreed with the committee.

REPORTING

The Chief Audit Executive will report to each meeting of the Audit and Risk Committee on:

- audits completed
- progress in implementing the annual audit work plan
- the implementation status of agreed internal and external audit recommendations.

The internal audit function will also report to the Audit and Risk Committee at least annually on the overall state of internal controls within the office and any systematic issues requiring management attention based on the work of the internal audit function and other assurance providers.

ADMINISTRATIVE ARRANGEMENTS

Any change to the position of the Chief Audit Executive or external service provider will be approved by the Commissioner in consultation with the Audit and Risk Committee.

The Chief Audit Executive will arrange for an internal review, at least annually, and a periodic independent review, at least every five years, of the efficiency and effectiveness of the operations of the internal audit function.

REVIEW OF THE CHARTER

The charter will be reviewed at least annually by the Audit and Risk Committee. Any substantive changes will be formally approved by the Commissioner on the recommendation of the Audit and Risk Committee.

CHARTER APPROVAL

Deirdre O'Donnell
Information Commissioner

16 June 2011