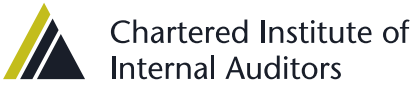
Public Sector Internal Audit Standards

Applying the IIA International Standards to the UK Public Sector

Issued by the Relevant Internal Audit Standard Setters:

In collaboration with:



Public Sector Internal Audit Standards

Applying the IIA International Standards to the UK Public Sector

ISBN 978 1 84508 356 4

Contents

SECTION 1

Introduction

A professional, independent and objective internal audit service is one of the key elements of good governance, as recognised throughout the UK public sector.

This document is therefore addressed to Accounting Officers, Accountable Officers, board and audit committee members, heads of internal audit, internal auditors, external auditors and other stakeholders such as chief financial officers and chief executives.

Framework overview

The Relevant Internal Audit Standard Setters (RIASS)[1] have adopted this common set of Public Sector Internal Audit Standards (PSIAS) from 1 April 2013. The PSIAS encompass the mandatory elements of the Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF) as follows:

- Definition of Internal Auditing
- Code of Ethics, and
- International Standards for the Professional Practice of Internal Auditing (including interpretations and glossary).

Additional requirements and interpretations for the UK public sector have been inserted in such a way as to preserve the integrity of the text of the mandatory elements of the IPPF.

The overarching principle borne in mind when all potential public sector interpretations and/or specific requirements were considered was that only the minimum number of additions should be made to the existing IIA Standards. The criteria against which potential public sector requirements were judged for inclusion were:

- where interpretation is required in order to achieve consistent application in the UK public sector
- where the issue is not addressed or not addressed adequately by the current IIA Standards, or
- where the IIA standard would be inappropriate or impractical in the context of public sector governance (taking into account, for example, any funding mechanisms, specific legislation etc).

At the same time, the following concepts were also considered of each requirement or interpretation being proposed:

- materiality
- relevance
- necessity, and
- integrity (the additional commentary does not cause inconsistency elsewhere).

1 The Relevant Internal Audit Standard Setters are: HM Treasury in respect of central government; the Scottish Government, the Department of Finance and Personnel Northern Ireland and the Welsh Government in respect of central government and the health sector in their administrations; the Department of Health in respect of the health sector in England (excluding Foundation Trusts); and the Chartered Institute of Public Finance and Accountancy in respect of local government across the UK.

Wherever reference is made to the International Standards for the Professional Practice of Internal Auditing, this is replaced by the PSIAS. Chief audit executives are expected to report conformance on the PSIAS in their annual report.

Purpose of the PSIAS

The objectives of the PSIAS are to:

- define the nature of internal auditing within the UK public sector
- set basic principles for carrying out internal audit in the UK public sector
- establish a framework for providing internal audit services, which add value to the organisation, leading to improved organisational processes and operations, and
- establish the basis for the evaluation of internal audit performance and to drive improvement planning.

Additional guidance is a matter for the RIASS.

Scope

The PSIAS apply to all internal audit service providers, whether in-house, shared services or outsourced.

All internal audit assurance and consulting services fall within the scope of the Definition of Internal Auditing (see section 3). The provision of assurance services is the primary role for internal audit in the UK public sector. This role requires the chief audit executive to provide an annual internal audit opinion based on an objective assessment of the framework of governance, risk management and control. Consulting services are advisory in nature and are generally performed at the specific request of the organisation, with the aim of improving governance, risk management and control and contributing to the overall opinion.

The Code of Ethics promotes an ethical, professional culture (see section 4). It does not supersede or replace internal auditors' own professional bodies' Codes of Ethics or those of employing organisations. Internal auditors must also have regard to the Committee on Standards of Public Life's *Seven Principles of Public Life.*

In common with the IIA IPPF on which they are based, the PSIAS comprise Attribute and Performance Standards. The Attribute Standards address the characteristics of organisations and parties performing internal audit activities. The Performance Standards describe the nature of internal audit activities and provide quality criteria against which the performance of these services can be evaluated. While the Attribute and Performance Standards apply to all aspects of the internal audit service, the Implementation Standards apply to specific types of engagements and are classified accordingly:

- Assurance (A) and
- Consulting (C) activities.

The Standards employ terms that have been given specific meanings that are included in the Glossary.

Key governance elements

Within the PSIAS, the terms 'board' and 'senior management' need to be interpreted in the context of the governance arrangements within each UK public sector organisation, as these arrangements vary in structure and terminology between sectors and from one organisation and the next within in the same sector.

It is also necessary for the chief audit executive to understand the role of the Accounting or Accountable Officer, Chief Financial Officer, chief executive, the audit committee and other key officers or relevant decision-making groups as well as how they relate to each other. Key relationships with these individuals and groups are defined for each internal audit service within its charter.

Applicability

The Relevant Internal Audit Standard Setters for the various parts of the UK public sector are shown below, along with the types of organisations in which the PSIAS should be applied.

SECTOR / RELEVANT INTERNAL AUDIT STANDARD SETTER	Central Government	NHS	Local Government
CIPFA			**UK** Local authorities. **England & Wales only** The Office of the Police & Crime Commissioner, constabularies, fire authorities, National Park authorities, joint committees and joint boards in the UK. **Scotland only** Strathclyde Partnership for Transport.
HM Treasury	**UK*** Government departments and their executive agencies and non-departmental public bodies.		
Department of Health		**England** Clinical Commissioning Groups. NHS Trusts.	

SECTOR / RELEVANT INTERNAL AUDIT STANDARD SETTER	Central Government	NHS	Local Government
Scottish Government	**Scotland** The Scottish Government, the Crown Office and Procurator Fiscal Service, Executive Agencies and non-ministerial departments, non-departmental public bodies, the Scottish Parliament Corporate Body and bodies sponsored / supported by the Scottish Parliament Corporate Body.	**Scotland** NHS Boards, Special NHS Boards, NHS Board partnership bodies in the public sector (eg joint ventures, Community Health Partnerships etc), NHS Board subsidiaries.	
Welsh Government	**Wales** The Welsh Government, National Assembly for Wales and Welsh Government sponsored bodies including commissioners.	**Wales** Health Boards and Trusts.	
Northern Ireland Assembly: Department of Finance and Personnel (NI)	Government departments, executive agencies, non-ministerial departments, non-departmental public bodies, NI health and social care bodies and other relevant sponsored bodies.		

* Unless the body falls under the jurisdiction of the devolved governments.

SECTION 3

Definition of Internal Auditing

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

SECTION 4

Code of Ethics

Public sector requirement

Internal auditors in UK public sector organisations (as set out in the Applicability section) must conform to the Code of Ethics as set out below. If individual internal auditors have membership of another professional body then he or she must also comply with the relevant requirements of that organisation.

The purpose of The Institute's Code of Ethics is to promote an ethical culture in the profession of internal auditing. A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about risk management, control and governance.

The Institute's Code of Ethics extends beyond the definition of internal auditing to include two essential components:

Components

1 Principles that are relevant to the profession and practice of internal auditing;

2 Rules of Conduct that describe behaviour norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

The Code of Ethics provides guidance to internal auditors serving others. 'Internal auditors' refers to Institute members and those who provide internal auditing services within the definition of internal auditing.

Applicability and Enforcement

This Code of Ethics applies to both individuals and entities that provide internal auditing services. For Institute members, breaches of the Code of Ethics will be evaluated and administered according to The Institute's Disciplinary Procedures. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable and therefore, the member liable to disciplinary action.

Public sector interpretation

The 'Institute' here refers to the IIA. Disciplinary procedures of other professional bodies and employing organisations may apply to breaches of this Code of Ethics.

1 Integrity

Principle

The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgement.

Rules of Conduct

Internal auditors:

1.1 Shall perform their work with honesty, diligence and responsibility.

1.2 Shall observe the law and make disclosures expected by the law and the profession.

1.3 Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organisation.

1.4 Shall respect and contribute to the legitimate and ethical objectives of the organisation.

2 Objectivity

Principle

Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined.

Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgements.

Rules of Conduct

Internal auditors:

2.1 Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organisation.

2.2 Shall not accept anything that may impair or be presumed to impair their professional judgement.

2.3 Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

3 Confidentiality

Principle

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

Rules of Conduct

Internal auditors:

3.1 Shall be prudent in the use and protection of information acquired in the course of their duties.

3.2 Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organisation.

4 Competency

Principle

Internal auditors apply the knowledge, skills and experience needed in the performance of internal auditing services.

Rules of Conduct

Internal auditors:

4.1 Shall engage only in those services for which they have the necessary knowledge, skills and experience.

4.2 Shall perform internal auditing services in accordance with the International Standards for the Professional Practice of Internal Auditing.

4.3 Shall continually improve their proficiency and effectiveness and quality of their services.

Public sector requirement

Internal auditors who work in the public sector must also have regard to the Committee on Standards of Public Life's *Seven Principles of Public Life*, information on which can be found at www.public-standards.gov.uk

Standards

Attribute Standards

1000 Purpose, Authority and Responsibility

The purpose, authority and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the *Definition of Internal Auditing,* the *Code of Ethics* and the *Standards.* The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

Interpretation:

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 organisation, including the nature of the chief audit executive's functional reporting relationship with the board; authorises access to records, personnel and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.

Public sector requirement

The internal audit charter must also:

- define the terms 'board' and 'senior management' for the purposes of internal audit activity;
- cover the arrangements for appropriate resourcing;
- define the role of internal audit in any fraud-related work; and
- include arrangements for avoiding conflicts of interest if internal audit undertakes non-audit activities.

1000.A1

The nature of assurance services provided to the organisation must be defined in the internal audit charter. If assurances are to be provided to parties outside the organisation, the nature of these assurances must also be defined in the internal audit charter.

1000.C1

The nature of consulting services must be defined in the internal audit charter.

1010 Recognition of the *Definition of Internal Auditing,* the *Code of Ethics* and the *Standards* in the Internal Audit Charter

The mandatory nature of the *Definition of Internal Auditing,* the *Code of Ethics* and the *Standards* must be recognised in the internal audit charter. The chief audit executive should discuss the *Definition of Internal Auditing,* the *Code of Ethics* and the *Standards* with senior management and the board.

1100 Independence and Objectivity

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

Interpretation:

Independence is the freedom from conditions that threaten the ability of the internal audit activity 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 board. This can be achieved through a dual-reporting relationship. 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.

1110 Organisational Independence

The chief audit executive must report to a level within the organisation that allows the internal audit activity to fulfil its responsibilities. The chief audit executive must confirm to the board, at least annually, the organisational independence of the internal audit activity.

Interpretation:

Organisational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board:

- approving the internal audit charter;
- approving the risk based internal audit plan;
- approving the internal audit budget and resource plan;
- receiving communications from the chief audit executive on the internal audit activity's performance relative to its plan and other matters;
- approving decisions regarding the appointment and removal of the chief audit executive;
- approving the remuneration of the chief audit executive; and
- making appropriate enquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.

Public sector requirement

The chief audit executive must report functionally to the board. The chief audit executive must also establish effective communication with, and have free and unfettered access to, the chief executive (or equivalent) and the chair of the audit committee.

Public sector interpretation

Governance requirements in the UK public sector would not generally involve the board approving the CAE's remuneration specifically. The underlying principle is that the independence of the CAE is safeguarded by ensuring that his or her remuneration or performance assessment is not inappropriately influenced by those subject to audit. In the UK public sector this can be achieved by ensuring that the chief executive (or equivalent) undertakes, countersigns, contributes feedback to or reviews the performance appraisal of the CAE and that feedback is also sought from the chair of the audit committee.

1110.A1

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

1111 Direct Interaction with the Board

The chief audit executive must communicate and interact directly with the board.

1120 Individual Objectivity

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

Interpretation:

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.

1130 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.

Interpretation:

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 board as described in the internal audit charter, as well as the nature of the impairment.

1130.A1

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.

1130.A2

Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

1130.C1

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

1130.C2

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.

Public sector requirement

Approval must be sought from the board for any significant additional consulting services not already included in the audit plan, prior to accepting the engagement.

1200 Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

1210 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.

Interpretation:

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.

Public sector requirement

The chief audit executive must hold a professional qualification (CMIIA, CCAB or equivalent) and be suitably experienced.

1210.A1

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.

1210.A2

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

1210.A3

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.

1210.C1

The chief audit executive must decline the consulting engagement or 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.

1220 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.

1220.A1

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.

1220.A2

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

1220.A3

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.

1220.C1

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.

1230 Continuing Professional Development

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

1300 Quality Assurance and Improvement Programme

The chief audit executive must develop and maintain a quality assurance and improvement programme that covers all aspects of the internal audit activity.

Interpretation:

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

1310 Requirements of the Quality Assurance and Improvement Programme

The quality assurance and improvement programme must include both internal and external assessments.

1311 Internal Assessments

Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity; and
- Periodic self-assessments or assessments by other persons within the organisation with sufficient knowledge of internal audit practices.

Interpretation:

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 *Definition of Internal Auditing,* the *Code of Ethics* and the *Standards.*

Periodic assessments are 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.

1312 External Assessments

External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organisation. The chief audit executive must discuss with the board:

- The form of external assessments;
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

Interpretation:

External assessments can be in the form of a full external assessment, or a self-assessment with independent external validation.

A qualified assessor or assessment team demonstrates competence in two areas: the professional practice of internal auditing and the external assessment process. Competence can be demonstrated through a mixture of experience and theoretical learning. Experience gained in organisations of similar size, complexity, sector or industry and technical issues is more valuable than less relevant experience. In the case of an assessment team, not all members of the team need to have all the competencies; it is the team as a whole that is qualified. The chief audit executive uses professional judgment when assessing whether an assessor or assessment team demonstrates sufficient competence to be qualified.

An independent assessor or assessment 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 organisation to which the internal audit activity belongs.

Public sector requirement

The chief audit executive must agree the scope of external assessments with an appropriate sponsor, eg the Accounting/Accountable Officer or chair of the audit committee as well as with the external assessor or assessment team.

1320 Reporting on the Quality Assurance and Improvement Programme

The chief audit executive must communicate the results of the quality assurance and improvement programme to senior management and the board.

Interpretation:

The form, content and frequency of communicating the results of the quality assurance and improvement programme is established through discussions with senior management and the board 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 assessor's or assessment team's evaluation with respect to the degree of conformance.

Public sector requirement

The results of the quality and assurance programme and progress against any improvement plans must be reported in the annual report.

1321 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 programme support this statement.

Interpretation:

The internal audit activity conforms with the Standards when it achieves the outcomes described in the *Definition of Internal Auditing, Code of Ethics* and *Standards.*

The results of the quality assurance and improvement programme include the results of both internal and external assessments. All internal audit activities will have the results of internal assessments. Internal audit activities in existence for at least five years will also have the results of external assessments.

1322 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 board.

Public sector requirement

Instances of non-conformance must be reported to the board. More significant deviations must be considered for inclusion in the governance statement.

Performance Standards

2000 Managing the Internal Audit Activity

The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organisation.

Interpretation:

The internal audit activity is effectively managed when:

- The results of the internal audit activity's work achieve the purpose and responsibility included in the internal audit charter;
- The internal audit activity conforms with the *Definition of Internal Auditing* and the *Standards;* and
- The individuals who are part of the internal audit activity demonstrate conformance with the *Code of Ethics* and the *Standards.*

The internal audit activity adds value to the organisation (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management and control processes.

2010 Planning

The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goals.

Interpretation:

The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organisation's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organisation. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organisation's business, risks, operations, programs, systems, and controls.

Public sector requirement

The risk-based plan must take into account the requirement to produce an annual internal audit opinion and the assurance framework. It must incorporate or be linked to a strategic or high-level statement of how the internal audit service will be delivered and developed in accordance with the internal audit charter and how it links to the organisational objectives and priorities.

2010.A1

The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

2010.A2

The chief audit executive must identify and consider the expectations of senior management, the board and other stakeholders for internal audit opinions and other conclusions.

2010.C1

The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value and improve the organisation's operations. Accepted engagements must be included in the plan.

2020 Communication and Approval

The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

2030 Resource Management

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

Interpretation:

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.

Public sector requirement

The risk-based plan must explain how internal audit's resource requirements have been assessed.

Where the chief audit executive believes that the level of agreed resources will impact adversely on the provision of the annual internal audit opinion, the consequences must be brought to the attention of the board.

2040 Policies and Procedures

The chief audit executive must establish policies and procedures to guide the internal audit activity.

Interpretation:

The form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work.

2050 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.

Public sector requirement

The chief audit executive must include in the risk-based plan the approach to using other sources of assurance and any work required to place reliance upon those other sources.

2060 Reporting to Senior Management and the Board

The chief audit executive must report periodically to senior management and the board 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 board.

Interpretation:

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

2070 External Service Provider and Organisational Responsibility for Internal Auditing

When an external service provider serves as the internal audit activity, the provider must make the organisation aware that the organisation has the responsibility for maintaining an effective internal audit activity.

Interpretation:

This responsibility is demonstrated through the quality assurance and improvement programme which assesses conformance with the *Definition of Internal Auditing,* the *Code of Ethics* and the *Standards.*

2100 Nature of Work

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

2110 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 organisation;
- Ensuring effective organisational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organisation; and
- Coordinating the activities of and communicating information among the board, external and internal auditors and management.

2110.A1

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

2110.A2

The internal audit activity must assess whether the information technology governance of the organisation supports the organisation's strategies and objectives.

2120 Risk Management

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

Interpretation:

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

- Organisational objectives support and align with the organisation's mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organisation's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organisation, enabling staff, management and the board to carry out their responsibilities.

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organisation's risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

2120.A1

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

- Achievement of the organisation's strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programmes;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures and contracts.

2120.A2

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

2120.C1

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

2120.C2

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

2120.C3

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

2130 Control

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

2130.A1

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

- Achievement of the organisation's strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programmes;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures and contracts.

2130.C1

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

2200 Engagement Planning

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

2201 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 governance, risk management and control processes compared to a relevant framework or model; and
- The opportunities for making significant improvements to the activity's governance, risk management and control processes.

2201.A1

When planning an engagement for parties outside the organisation, 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.

2201.C1

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.

2210 Engagement Objectives

Objectives must be established for each engagement.

2210.A1

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.

2210.A2

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

2210.A3

Adequate criteria are needed to evaluate governance, risk management and controls. Internal auditors must ascertain the extent to which management and/or the board 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 and/or the board to develop appropriate evaluation criteria.

Public sector interpretation

In the public sector, criteria are likely to include value for money.

2210.C1

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

2210.C2

Consulting engagement objectives must be consistent with the organisation's values, strategies and objectives.

2220 Engagement Scope

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

2220.A1

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

2220.A2

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.

2220.C1

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.

2220.C2

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

2230 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.

2240 Engagement Work Programme

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

2240.A1

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

2240.C1

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

2300 Performing the Engagement

Internal auditors must identify, analyse, evaluate and document sufficient information to achieve the engagement's objectives.

2310 Identifying Information

Internal auditors must identify sufficient, reliable, relevant and useful information to achieve the engagement's objectives.

Interpretation:

Sufficient information is factual, adequate and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Reliable information is the best attainable information through the use of appropriate engagement techniques. Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement. Useful information helps the organisation meet its goals.

2320 Analysis and Evaluation

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

2330 Documenting Information

Internal auditors must document relevant information to support the conclusions and engagement results.

2330.A1

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.

2330.A2

The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organisation's guidelines and any pertinent regulatory or other requirements.

2330.C1

The chief audit executive must develop policies 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 the organisation's guidelines and any pertinent regulatory or other requirements.

2340 Engagement Supervision

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

Interpretation:

The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The chief audit executive has overall responsibility for supervising the engagement, whether performed by or for the internal audit activity, but may designate appropriately experienced members of the internal audit activity to perform the review. Appropriate evidence of supervision is documented and retained.

2400 Communicating Results

Internal auditors must communicate the results of engagements.

2410 Criteria for Communicating

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

2410.A1

Final communication of engagement results must, where appropriate, contain internal auditors' opinion and/or conclusions. When issued, an opinion or conclusion must take account of the expectations of senior management, the board and other stakeholders and must be supported by sufficient, reliable, relevant and useful information.

Interpretation:

Opinions at the engagement level may be ratings, conclusions or other descriptions of the results. Such an engagement may be in relation to controls around a specific process, risk or business unit. The formulation of such opinions requires consideration of the engagement results and their significance.

2410.A2

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

2410.A3

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

2410.C1

Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

2420 Quality of Communications

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

Interpretation:

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 engagement client and the organisation 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.

2421 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.

2430 Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"

Internal auditors may report that their engagements are "conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing",* only if the results of the quality assurance and improvement programme support the statement.

2431 Engagement Disclosure of Nonconformance

When nonconformance with the *Definition of Internal Auditing,* the *Code of Ethics* or the *Standards* impacts a specific engagement, communication of the results must disclose the:

- Principle or rule of conduct of the *Code of Ethics* or Standard(s) with which full conformance was not achieved;
- Reason(s) for nonconformance; and
- Impact of nonconformance on the engagement and the communicated engagement results.

2440 Disseminating Results

The chief audit executive must communicate results to the appropriate parties.

Interpretation:

The chief audit executive is responsible for reviewing and approving the final engagement communication before issuance and deciding to whom and how it will be disseminated. When the chief audit executive delegates these duties, he or she retains overall responsibility.

2440.A1

The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

2440.A2

If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organisation the chief audit executive must:

- Assess the potential risk to the organisation;
- Consult with senior management and/ or legal counsel as appropriate; and
- Control dissemination by restricting the use of the results.

2440.C1

The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

2440.C2

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

2450 Overall Opinions

When an overall opinion is issued, it must take into account the expectations of senior management, the board and other stakeholders and must be supported by sufficient, reliable, relevant and useful information.

Interpretation:

The communication will identify:

- The scope including the time period to which the opinion pertains;
- Scope limitations;
- Consideration of all related projects including the reliance on other assurance providers;
- The risk or control framework or other criteria used as a basis for the overall opinion; and
- The overall opinion, judgment or conclusion reached.

The reasons for an unfavourable overall opinion must be stated.

Public sector requirement

The chief audit executive must deliver an annual internal audit opinion and report that can be used by the organisation to inform its governance statement.

The annual internal audit opinion must conclude on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control.

The annual report must incorporate:

- the opinion;
- a summary of the work that supports the opinion; and
- a statement on conformance with the Public Sector Internal Audit Standards and the results of the quality assurance and improvement programme.

2500 Monitoring Progress

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1

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.

2500.C1

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

2600 Communicating the Acceptance of Risks

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organisation, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

Interpretation:

The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk.

Glossary

Add Value

The internal audit activity adds value to the organisation (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management and control processes.

Adequate Control

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

Public sector definition: Assurance Framework

This is the primary tool used by a board to ensure that it is properly informed on the risks of not meeting its objectives or delivering appropriate outcomes and that it has adequate assurances on the design and operation of the systems in place to mitigate those risks.

Assurance Services

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

Public sector definition: Audit Committee

The governance group charged with independent assurance of the adequacy of the risk management framework, the internal control environment and the integrity of financial reporting.

Board

The highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organisation. Typically, this includes an independent group of directors (eg a board of directors, a supervisory board or a board of governors or trustees). If such a group does not exist, the 'board' may refer to the head of the organisation. 'Board' may refer to an audit committee to which the governing body has delegated certain functions.

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 organisation; 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 describes a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the *Definition of Internal Auditing,* the *Code of Ethics* and the *Standards.* The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title of the chief audit executive may vary across organisations.

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 organisation. 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 organisation'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 board 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 board and management regarding the importance of control within the organisation. 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 (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organisation is willing to accept.

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 Opinion

The rating, conclusion and/or other description of results of an individual internal audit engagement, relating to those aspects within the objectives and scope of the engagement.

Engagement Work Programme

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 organisation 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 board to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives.

Public sector definition: Governance Statement

The mechanism by which an organisation publicly reports on its governance arrangements each year.

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 the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.

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 enterprise's information technology supports the organisation'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 an organisation's operations. The internal audit activity helps an organisation 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.

Public sector interpretation

Only the mandatory elements apply for the purposes of the Public Sector Internal Audit Standards.

Public sector interpretation: International Standards for the Professional Practice of Internal Auditing

The Public Sector Internal Audit Standards take the place of the International Standards where applicable.

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 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.

Overall Opinion

The rating, conclusion and/or other description of results provided by the chief audit executive addressing, at a broad level, governance, risk management and/or control processes of the organisation. An overall opinion is the professional judgement of the chief audit executive based on the results of a number of individual engagements and other activities for a specific time interval.

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 an organisation 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 organisation'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 programmes, specialised audit utilities and computer-assisted audit techniques (CAATs).