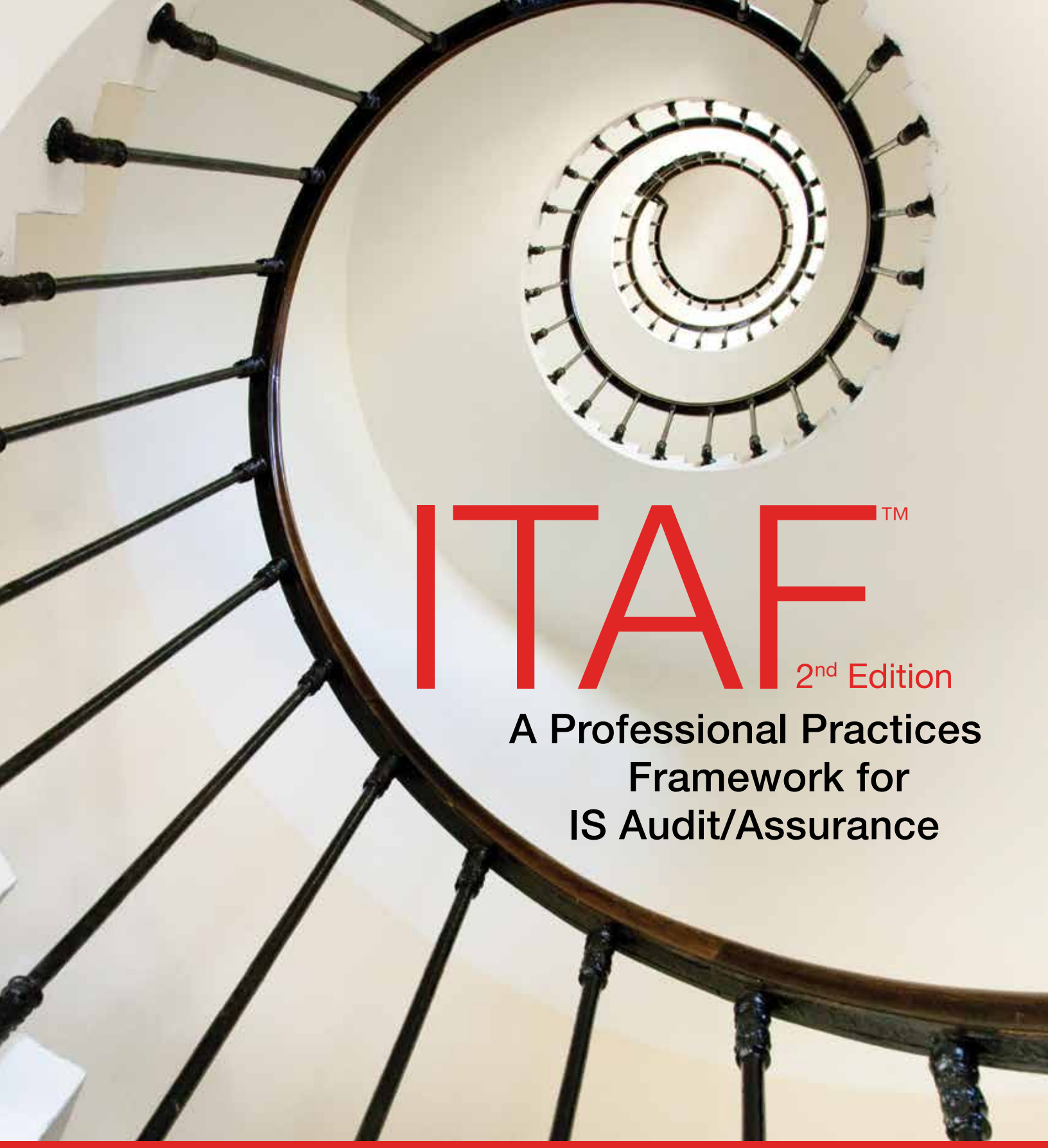

ITAF™

2nd Edition

A Professional Practices Framework for IS Audit/Assurance

ISACA®

Trust in, and value from, information systems

About ISACA®
With more than 100,000 constituents in 180 countries, ISACA *(www.isaca.org)* is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT framework. COBIT helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA has designed and created *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 2nd Edition* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *Info@isaca.org*
Web site: *www.isaca.org*

Provide Feedback: *www.isaca.org/ITAF*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

Acknowledgements

ISACA wishes to recognise:

ISACA Board of Directors
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, International President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Carselle, CISA, CGEIT, CRISC, Wal-Mart, Mexico, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal Raj, CISA, CISM, CGEIT, CFE. CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Past International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Director
Krysten McCabe, CISA, The Home Depot, USA, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich , Australia, Director

Credentialing and Career Management Board
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Chairman
Bernard Battistin, CISA, CMA, Office of the Auditor General of Canada, Canada
Richard Brisebois, CISA, CGA, Canada
Terry Chrisman, CGEIT, CRISC, GE Money, USA
Erik Friebolin, CISA, CISM, CRISC, CISSP, PCI-QSA, ITIL, USA
Frank Nielsen, CISA, CGEIT, CCSA,CIA, Nordea, Denmark
Hitoshi Ota, CISA, CISM, CGEIT, CRISC, CIA, Mizuho Corporate Bank, Japan
Carmen Ozores Fernandes, CISA, CRISC, Brazil
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, USA

Professional Standards and Career Management Committee
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, USA, Chairman
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP, HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA, Myers and Stauffer LLC, USA
Alisdair McKenzie, CISA, CISSP, ITCP, I S Assurance Services, New Zealand
Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP, University of North Texas, USA
Katsumi Sakagawa, CISA, CRISC, PMP, JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA, NATO, Belgium
Timothy Smith, CISA, CISSP, CPA, LPL Financial, USA
Todd Weinman, CPS, The Weinman Group, USA

Table of Contents

Introduction

ITAF is a comprehensive and good-practice-setting reference model that:
- Establishes standards that address IS audit and assurance professional roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements
- Defines terms and concepts specific to IS assurance
- Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments

ITAF is focused on ISACA material and provides a single source through which IS audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programmes, and develop effective reports.

While ITAF incorporates existing ISACA IS audit and assurance standards and guidance, it has been designed to be a living document. As new guidance is developed and issued, it will be indexed within the framework. Current ISACA guidance has been mapped to the framework.

The ISACA Professional Standards and Career Management Committee is committed to wide consultation in the preparation of IS audit and assurance standards and guidance. Prior to issuing any document, an exposure draft is issued internationally for general public comment. An online questionnaire accompanies the exposure draft and will be available at *www.isaca.org/standardexposure*. Comments may also be submitted via email to the attention of the director of professional standards development at standards@isaca.org.

Frequently asked questions:
- **To whom does ITAF apply?** ITAF applies to individuals who act in the capacity of IS audit and assurance professionals and are engaged in providing assurance over some components of IS applications and infrastructure. However, care has been taken to design these standards, guidelines, and tools and techniques in a manner that may also be useful and provide benefits to a wider audience, including users of IS audit and assurance reports.
- **When should ITAF be used?** The application of the framework is a prerequisite to conducting IS audit and assurance work. The standards are mandatory. The guidelines, tools and techniques are designed to provide non-mandatory assistance in performing assurance work.
- **Where should ITAF IS audit and assurance standards and related guidance be used?** ITAF's design recognises that IS audit and assurance professionals are faced with different requirements and types of assignments—ranging from leading an IS-focused audit to contributing to a financial or operational audit. ITAF is applicable to any formal IS audit or assessment engagement.
- **Does ITAF address requirements for consultative and advisory work?** In addition to assessment work, IS audit and assurance professionals frequently undertake consultative and advisory engagements for their employers or on behalf of clients. These assignments usually result in an assessment of a particular area; identification of issues, concerns or weaknesses; and the development of recommendations. For a number of reasons, including nature of the work, scope of the engagement, independence and degree of testing, the work is not considered an audit and, therefore, the IS audit and assurance professional does not issue a formal audit report. ITAF has not been designed to address specific requirements with respect to this consultative and advisory work.

Organisation

ITAF IS audit and assurance standards are divided into three categories:
- **General standards (1000 series)**—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- **Performance standards (1200 series)**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care
- **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated

ITAF IS audit and assurance guidelines provide the IS audit and assurance professional with information and direction about an IS audit or assurance area. In line with the three categories of standards outlined above, guidelines focus on the various audit approaches, methodologies and related material to assist in planning, executing, assessing, testing and reporting on IS processes, controls and related IS audit or assurance initiatives. Guidelines also help clarify the relationship between enterprise activities and initiatives, and those undertaken by IT.

ITAF IS audit and assurance guidelines are also divided into three categories:
- **General guidelines (2000 series).**
- **Performance guidelines (2200 series)**
- **Reporting guidelines (2400 series)**

Tools and techniques, section 3000, provide specific information on various methodologies, tools and templates—and provide direction in their application and use to operationalise the information provided in the guidance. Note that the tools and techniques take a variety of forms, such as discussion documents, technical direction, white papers, audit programmes or books—e.g., the ISACA publication on SAP, which provides guidance on enterprise resource planning (ERP) systems.

In line with ITAF's design as a living document, section numbers intentionally include gaps where future guidance may be inserted.

Using ITAF

The standards are mandatory in all cases. The term "shall" indicates "must". Any deviations must be addressed prior to completion of the IS audit or assurance engagement.

The guidelines are not mandatory—but adhering to them is strongly recommended. Although they do allow IS audit and assurance professionals a degree of application freedom, professionals must be able to defend and justify any significant deviation from the guidelines or the omission of relevant sections of the guidance in the conduct of IS audit and assurance engagements. This is particularly true if the engagement is more at the IS audit level. Not all guidelines will be applicable in all situations, but they should always be considered.

Tools and techniques represent supplementary material and information that supports the guidance. In some cases, the techniques present alternatives or even a range of techniques, many of which may be applicable. Techniques should be selected only if they are suitable and appropriate and result in the IS audit and assurance professional obtaining appropriate, relevant, objective and unbiased information.

Complete information regarding ISACA IS audit and assurance standards and guidelines can be found at *www.isaca.org/standards*.

The IS audit or assurance process involves the performance of specific procedures to provide an appropriate level of assurance about the subject matter. IS audit and assurance professionals undertake assignments designed to provide assurance at varying levels, ranging from review to attestation or examination.

Each IS audit or assurance assignment must adhere to prescribed standards in terms of whether individuals are qualified to perform the work, how the work is performed, what work is performed and how the findings will be reported based on various characteristics of the assignment and the nature of the results obtained. If the engagement is to be performed by one individual, that individual must possess the skill and knowledge required to complete the engagement. If more than one individual is performing the engagement, the team needs to collectively possess the skill and knowledge to perform the work.

Several critical hypotheses are inherent in any IS audit or assurance assignment, including:
- The subject matter is identifiable and subject to audit.
- There is a high probability of successful completion of the project.
- The approach and methodology are free from bias.
- The project is of sufficient scope to meet the IS audit or assurance objectives.
- The project will lead to a report that is objective and that will not mislead the reader.

Standards Issued by Other Standard-setting Bodies

While the ITAF standards provide IS audit and assurance professionals with the guidance and direction required, situations may arise in which they may be required to use regulatory standards issued by another organisation.

The IS audit and assurance professional may:
- Use ITAF standards in conjunction with professional standards issued by other authoritative bodies
- Cite the use of other standards apart from ITAF standards in their reports

When the IS audit and assurance professional is using standards other than the ITAF standards, care should be taken to ensure that conflicts do not arise between the standards.

When the IS audit and assurance professional has cited compliance with ITAF standards, and inconsistencies exist between ITAF and other standards cited, the IS audit and assurance professional should use ITAF standards as the prevailing standards for conducting reviews and reporting the results unless the other standards are regulatory requirements.

Terms and Definitions

Throughout this document, common words are used with specific meaning. Accordingly, to ensure the words and their meaning within the context of this document are understood and consistently applied, a complete glossary is available on the ISACA web site, *www.isaca.org/glossary*.

ISACA Code of Professional Ethics

ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.
4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
6. Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.

1. IS Audit and Assurance Standards

As indicated in the introduction, the standards in ITAF—general, performance and reporting—must be followed in all circumstances. In addition, the standards contain key aspects designed to assist the IS audit and assurance professional; thus, information within the standard where compliance is obligatory has been identified in **bold**. ITAF standards are periodically reviewed for continual improvement and amended as necessary to keep pace with the evolving challenges in the IS audit and assurance profession.

Standards Statements

The mandatory standards statements have been inserted here for easy reference.

General

1001 Audit Charter

1001.1 The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.

1001.2 The IS audit and assurance function shall have the audit charter agreed upon and approved at an appropriate level within the enterprise.

1002 Organisational Independence

1002.1 The IS audit and assurance function shall be independent of the area or activity being reviewed to permit objective completion of the audit and assurance engagement.

1003 Professional Independence

1003.1 IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.

1004 Reasonable Expectation

1004.1 IS audit and assurance professionals shall have reasonable expectation that the engagement can be completed in accordance with the IS audit and assurance standards and, where required, other appropriate professional or industry standards" or applicable regulations and result in a professional opinion or conclusion.

1004.2 IS audit and assurance professionals shall have reasonable expectation that the scope of the engagement enables conclusion on the subject matter and addresses any restrictions.

1004.3 IS audit and assurance professionals shall have reasonable expectation that management understands its obligations and responsibilities with respect to the provision of appropriate, relevant and timely information required to perform the engagement.

1005 Due Professional Care

1005.1 IS audit and assurance professionals shall exercise due professional care, including observance of applicable professional audit standards, in planning, performing and reporting on the results of engagements.

1006 Proficiency

1006.1 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate skills and proficiency in conducting IS audit and assurance engagements and be professionally competent to perform the work required.

1006.2 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate knowledge of the subject matter.

1006.3 IS audit and assurance professionals shall maintain professional competence through appropriate continuing professional education and training.

1007 Assertions

1007.1 IS audit and assurance professionals shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

1008 Criteria

1008.1 IS audit and assurance professionals shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, measureable, understandable, widely recognised, authoritative and understood by, or available to, all readers and users of the report.

1008.2 IS audit and assurance professionals shall consider the source of the criteria and focus on those issued by relevant authoritative bodies before accepting lesser-known criteria.

Performance

1201 Engagement Planning

1201.1 IS audit and assurance professionals shall plan each IS audit and assurance engagement to address:
- Objective(s), scope, timeline and deliverables
- Compliance with applicable laws and professional auditing standards
- Use of a risk-based approach, where appropriate
- Engagement-specific issues
- Documentation and reporting requirements

1201.2 IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the:
- Engagement nature, objectives, timeline and resource requirements
- Timing and extent of audit procedures to complete the engagement

1202 Risk Assessment in Planning

1202.1 The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources.

1202.2 IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements.

1202.3 IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.

1203 Performance and Supervision

1203.1 IS audit and assurance professionals shall conduct the work in accordance with the approved IS audit plan to cover identified risk and within the agreed-on schedule.

1203.2 IS audit and assurance professionals shall provide supervision to IS audit staff whom they have supervisory responsibility for so as to accomplish audit objectives and meet applicable professional audit standards.

1203.3 IS audit and assurance professionals shall accept only tasks that are within their knowledge and skills or for which they have a reasonable expectation of either acquiring the skills during the engagement or achieving the task under supervision.

1203.4 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

1203.5 IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions.

1203.6 IS audit and assurance professionals shall identify and conclude on findings.

1204 Materiality

1204.1 IS audit and assurance professionals shall consider potential weaknesses or absences of controls while planning an engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness.

1204.2 IS audit and assurance professionals shall consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures.

1204.3 IS audit and assurance professionals shall consider the cumulative effect of minor control deficiencies or weaknesses and whether the absence of controls translates into a significant deficiency or a material weakness.

1204.4 IS audit and assurance professionals shall disclose the following in the report:
- Absence of controls or ineffective controls
- Significance of the control deficiency
- Likelihood of these weaknesses resulting in a significant deficiency or material weakness

1205 Evidence

1205.1 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results.

1205.2 IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives

1206 Using the Work of Other Experts

1206.1 IS audit and assurance professionals shall consider using the work of other experts for the engagement, where appropriate.

1206.2 IS audit and assurance professionals shall assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.

1206.3 IS audit and assurance professionals shall assess, review and evaluate the work of other experts as part of the engagement, and document the conclusion on the extent of use and reliance on their work.

1206.4 IS audit and assurance professionals shall determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives, and clearly document the conclusion.

1206.5 IS audit and assurance professionals shall determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.

1206.6 IS audit and assurance professionals shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.

1206.7 IS audit and assurance professionals shall provide an appropriate audit opinion or conclusion, and include any scope limitation where required evidence is not obtained through additional test procedures.

1207 Irregularity and Illegal Acts

1207.1 IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement.

1207.2 IS audit and assurance professionals shall maintain an attitude of professional scepticism during the engagement.

1207.3 IS audit and assurance professionals shall document and communicate any material irregularities or illegal act to the appropriate party in a timely manner.

Reporting

1401 Reporting

1401.1 IS audit and assurance professionals shall provide a report to communicate the results upon completion of the engagement including:

- Identification of the enterprise, the intended recipients and any restrictions on content and circulation
- The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed
- The findings, conclusions, and recommendations
- Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement
- Signature, date and distribution according to the terms of the audit charter or engagement letter

1401.2 IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient and appropriate audit evidence

1402 Follow-up Activities

1402.1 IS audit and assurance professionals shall monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations.

General Standards

General standards are the guiding principles under which the IS audit and assurance professional operates. They apply to the conduct of all assignments and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care, as well as knowledge, competency and skill.

In conducting an IS audit or assurance assignment the IS audit and assurance professional will be required to assess number of key decisions regarding the subject matter to be audited and the criteria against which the subject matter is to be assessed. In doing so, the IS audit and assurance professional will need to consider the benchmarks against which the assignment is to be conducted (standards) and against which the subject matter is to be assessed (criteria).

The general standards are:
1001 Audit Charter
1002 Organisational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency
1007 Assertions
1008 Criteria

The standards are included here in their entirety. Underlined words are defined in the Terms section. For links to the individual standards, visit *www.isaca.org/standard*.

1001 Audit Charter

Statements

1001.1 The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.

1001.2 The IS audit and assurance function shall have the audit charter agreed upon and approved at an appropriate level within the enterprise.

Key Aspects

The IS audit and assurance function should:

- Prepare an audit charter to define the activities of the internal IS audit and assurance function with enough detail to communicate:
  - The authority, purpose, responsibilities and limitations of the IS audit and assurance function
  - The independence and accountability of the IS audit and assurance function
  - Roles and responsibilities of the auditee during the IS audit engagement or assurance engagement
  - Professional standards that the IS audit and assurance professional will follow in the conduct of IS audit and assurance engagements
- Review the audit charter at least annually, or more frequently if the responsibilities change.
- Update the audit charter as needed to ensure that the purpose and responsibilities have been and remain documented appropriately.
- Formally communicate the audit charter to the auditee for each IS audit or assurance engagement.

Terms

Term	Definition
Assurance engagement	An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the enterprise. Scope note: Examples may include financial, performance, compliance and system security engagements
Audit charter	A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal audit activity. The charter should: • Establish the internal audit function's position within the enterprise • Authorise access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagements • Define the scope of the audit function's activities
Audit engagement	A specific audit assignment, task or review activity, such as an audit, control self-assessment review, fraud examination or consultancy. An audit engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.
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. Independence includes Independence of mind and Independence in appearance.

Linkage to Guidelines

Type	Title
Guideline	2001 Audit Charter

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1002 Organisational Independence

Statements

1002.1 The IS audit and assurance function shall be independent of the area or activity being reviewed to permit objective completion of the audit and assurance engagement.

Key Aspects

The IS audit and assurance function should:

- Report to a level within the auditee organisation that provides organisational independence and enables the IS audit and assurance function to perform its responsibilities without interference.
- Disclose the details of the impairment to the appropriate parties if independence is impaired in fact or appearance.
- Avoid non-audit roles in IS initiatives that require assumption of management responsibilities as such roles could impair future independence.
- Address independence and accountability of the audit function in its charter and/or engagement letter.

Terms

Term	Definition
Impairment	A condition that causes a weakness or diminished ability to execute audit objectives Impairment to organisational independence and individual objectivity may include personal conflict of interest; scope limitations; restrictions on access to records, personnel, equipment or facilities; and resource limitations (such as funding or staffing).
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. Independence includes Independence of mind and Independence in appearance.
Independence in appearance	The avoidance of facts and circumstances that are so significant that a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances, that a firm, audit function or a member of the audit team's integrity, objectivity or professional scepticism has been compromised.
Independence of mind	The state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgement, thereby allowing an individual to act with integrity and exercise objectivity and professional scepticism.
Objectivity	The ability to exercise judgement, express opinions and present recommendations with impartiality

Linkage to Guidelines

Type	Title
Guideline	2002 Organisational Independence

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1003 Professional Independence

Statements

1003.1 IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.

Key Aspects

IS audit and assurance professionals should:

- Conduct the IS audit or assurance engagement with an impartial and unbiased frame of mind in addressing assurance issues and reaching conclusions.
- Be independent in fact, but also appear to be independent at all times.
- Disclose the details of impairment to the appropriate parties if independence is impaired in fact or appearance.
- Assess independence regularly with management and the audit committee, if one is in place.
- Avoid non-audit roles in IS initiatives that require assumption of management responsibilities because such roles could impair future independence.

Terms

Term	Definition
Impairment	A condition that causes a weakness or diminished ability to execute audit objectives Impairment to organisational independence and individual objectivity may include personal conflict of interest; scope limitations; restrictions on access to records, personnel, equipment or facilities; and resource limitations (such as funding or staffing).
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. Independence includes Independence of mind and Independence in appearance.
Independence in appearance	The avoidance of facts and circumstances that are so significant that a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances, that a firm, audit function or a member of the audit team's integrity, objectivity or professional scepticism has been compromised.
Independence of mind	The state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgement, thereby allowing an individual to act with integrity and exercise objectivity and professional scepticism.
Objectivity	The ability to exercise judgement, express opinions and present recommendations with impartiality

Linkage to Guidelines

Type	Title
Guideline	2003 Professional Independence

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1004 Reasonable Expectation

Statements

1004.1 IS audit and assurance professionals shall have reasonable expectation that the engagement can be completed in accordance with the IS audit and assurance standards and, where required, other appropriate professional or industry standards or applicable regulations and result in a professional opinion or conclusion.

1004.2 IS audit and assurance professionals shall have reasonable expectation that the scope of the engagement enables conclusion on the subject matter and addresses any restrictions.

1004.3 IS audit and assurance professionals shall have reasonable expectation that management understands its obligations and responsibilities with respect to the provision of appropriate, relevant and timely information required to perform the engagement.

Key Aspects

IS audit and assurance professionals should:

- Undertake the IS audit or assurance engagement only if the work can be successfully completed in accordance with professional standards.
- Undertake the IS audit or assurance engagement only if the subject matter of the engagement can be assessed against relevant criteria.
- Review the scope of the IS audit or assurance engagement to determine that it is clearly documented and permits a conclusion to be drawn on the subject matter.
- Identify and address any restrictions being placed upon the engagement to be performed, including access to appropriate, relevant and timely information.
- Consider whether the scope is sufficient to permit an auditor's opinion to be expressed on the subject matter. Scope limitations may occur when information required to complete the engagement is unavailable, when the time frame included in the IS audit or assurance engagement is insufficient or when management attempts to limit the scope to selected areas. In such cases, other types of engagements may be considered such as support for audited financial statements, reviews of controls, compliance with required standards and practices or compliance with agreements, licences, legislation and regulation.

Terms

Term	Definition
Auditor's opinion	A formal statement expressed by the IS audit or assurance professional that describes the scope of the audit, the procedures used to produce the report and whether or not the findings support that the audit criteria have been met. The types of opinions are: • **Unqualified opinion**—Notes no exceptions or none of the exceptions noted aggregate to a significant deficiency • **Qualified opinion**—Notes exceptions aggregated to a significant deficiency (but not a material weakness) • **Adverse opinion**—Notes one or more significant deficiencies aggregating to a material weakness Note: A disclaimer of opinion it is issued when the auditor is unable to obtain sufficient appropriate audit evidence on which to base an opinion or if it is impossible to form an opinion due to the potential interactions of multiple uncertainties and their possible cumulative impact.

Linkage to Guidelines

Type	Title
Guideline	2004 Reasonable Expectation

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1005 Due Professional Care

Statements

1005.1 IS audit and assurance professionals shall exercise due professional care, including observance of applicable professional audit standards, in planning, performing and reporting on the results of engagements.

Key Aspects

IS audit and assurance professionals should:

- Perform engagements with integrity and care.
- Demonstrate sufficient understanding and competency to achieve engagement objectives.
- Maintain professional scepticism throughout the engagement.
- Maintain professional competency by keeping informed of and complying with developments in professional standards.
- Communicate with team members their roles and responsibilities and ensure the team's adherence to the appropriate standards in conducting engagements.
- Address all concerns encountered with regard to the application of standards during the conduct of the engagement.
- Maintain effective communications with relevant stakeholders throughout the engagement.
- Take reasonable measures to protect information obtained or derived during the engagement from inadvertent release or disclosure to unauthorised parties.
- Conduct all engagements with the concept of reasonable assurance in mind. The level of testing will vary with the type of engagement.

Note: Due professional care implies reasonable care and competence, not infallibility or extraordinary performance.

Terms

Term	Definition
Professional scepticism	An attitude that includes a questioning mind and a critical assessment of audit evidence. Source: American Institute of Certified Public Accountants (AICPA) AU 230.07

Linkage to Guidelines

Type	Title
Guideline	2005 Due Professional Care

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1006 Proficiency

Statements

1006.1 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate skills and proficiency in conducting IS audit and assurance engagements and be professionally competent to perform the work required.

1006.2 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate knowledge of the subject matter.

1006.3 IS audit and assurance professionals shall maintain professional competence through appropriate continuing professional education and training.

Key Aspects

IS audit and assurance professionals should:

- Demonstrate that sufficient professional competencies (skills, knowledge and experience relevant to the planned engagement) are available prior to the commencement of the work.
- Assess alternative means of acquiring the skills, including sub-contracting, outsourcing a portion of the tasks, delaying the assignment until such skills are available or otherwise ensuring the appropriate skills are available.
- Ensure that team members who neither hold a CISA nor other relevant professional designation and are involved in the IS audit and assurance engagement, have sufficient formal education, training and work experience.
- Provide reasonable assurance when leading a team to conduct an IS audit or assurance engagement that all team members have the appropriate level of professional competency for the work they perform.
- Have sufficient knowledge of key areas to enable conduct of the IS audit or assurance engagement effectively and efficiently, along with any specialists used and other team members.
- Meet continuing professional education or development requirements of CISA or other relevant professional designations.
- Update professional knowledge continually through educational courses, seminars, conferences, webcasts and on-the-job training to provide a level of professional service commensurate with the requirements of the IS audit or assurance role.

Terms

Term	Definition
Competence	The ability to perform a specific task, action or function successfully
Proficiency	Possessing skill and experience

Linkage to Guidelines

Type	Title
Guideline	2006 Proficiency

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1007 Assertions

Statements

1007.1 IS audit and assurance professionals shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

Key Aspects

IS audit and assurance professionals should:

- Evaluate the criteria against which the subject matter is to be assessed to assure they support the assertions.
- Determine whether the assertions are auditable and supported by corroborating information.
- Determine whether the assertions are based on criteria that are appropriately determined and subject to objective and measurable analysis.
- Where assertions have been developed by management, ensure that, when compared to other standards of authoritative pronouncements that the assertions are sufficient with respect to what a knowledgeable reader or user would expect.
- Where assertions have been developed by third parties who operate controls on behalf of the enterprise, ensure that the assertions are verified and accepted by management.
- Report either directly against the subject matter (direct report) or against an assertion about the subject matter (indirect report).
- Form a conclusion about each assertion, based on the aggregate of the findings against criteria along with professional judgment.

Terms

Term	Definition
Assertion	Any formal declaration or set of declarations about the subject matter made by management. Assertions should usually be in writing and commonly contain a list of specific attributes about the specific subject matter or about a process involving the subject matter.

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1008 Criteria

Statements

1008.1 IS audit and assurance professionals shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, measureable, understandable, widely recognised, authoritative and understood by, or available to, all readers and users of the report.

1008.2 IS audit and assurance professionals shall consider the source of the criteria and focus on those issued by relevant authoritative bodies before accepting lesser-known criteria.

Key Aspects

IS audit and assurance professionals should:

- Consider the selection of criteria carefully and be able to justify the selection.
- Use professional judgement in ensuring that, if applied, the use of the criteria will enable the development of a fair and objective opinion or conclusion that will not mislead the reader or user. It is recognised that management might put forth criteria that do not meet all of the requirements.
- Consider the suitability and availability of criteria in determining the engagement requirements.
- Where criteria are not readily available, incomplete or subject to interpretation, include a description and any other information necessary to ensure that the report is fair, objective and understandable, and the context in which the criteria are used is included in the report.

The suitability and appropriateness of subject matter assessment criteria should be assessed against the following five suitability criteria:

- **Objectivity**—Criteria should be free from bias that may adversely impact the professional's findings and conclusions, and, accordingly, may mislead the user of the report.
- **Completeness**—Criteria should be sufficiently complete so that all criteria that could affect the professional's conclusions about the subject matter are identified and used in the conduct of the IS audit or assurance engagement.
- **Relevance**—Criteria should be relevant to the subject matter and contribute to findings and conclusions that meet the objectives of the IS audit or assurance engagement.
- **Measurability**—Criteria should permit consistent measurement of the subject matter and the development of consistent conclusions when applied by different professionals in similar circumstances.
- **Understandability**—Criteria should be communicated clearly and not be subject to significantly different interpretations by intended users.

The acceptability of criteria is affected by the availability of the criteria to users of the professional's report, so that users understand the basis of the assurance activity and the relevance of the findings and conclusions. Sources may include those that are:

- **Recognised**—Criteria should be sufficiently well recognised so that their use is not questioned by intended users.
- **Authoritative**—Criteria should be sought that reflect authoritative pronouncements within the area and are appropriate for the subject matter. For example, authoritative pronouncements may come from professional bodies, industry groups, government and regulators.
- **Publicly available**—Criteria should be available to the users of the professional's report. Examples include standards developed by professional accounting and audit bodies such as ISACA, International Federation of Accountants (IFAC), and other recognised government or professional bodies.
- **Available to all users**—Where criteria are not publicly available, they should be communicated to all users through 'assertions' that form part of the professional's report. Assertions consist of statements about the subject matter that meet the requirements of 'suitable criteria' so that they can be audited.

1008 Criteria *(cont.)*

Key Aspects (cont.)

In addition to suitability and availability, the selection of IS assurance criteria should also consider their source, in terms of their use and the potential audience. For example, when dealing with government regulations, criteria based on assertions developed from the legislation and regulations that apply to the subject matter may be most appropriate. In other cases, industry or trade association criteria may be relevant. Possible criteria sources, listed in order of consideration, are:

- **Criteria established by ISACA**—These are publicly available criteria and standards that have been exposed to peer review and a thorough due-diligence process by recognised international experts in IT governance, control, security and assurance.
- **Criteria established by other bodies of experts**—Similar to ISACA standards and criteria, these are relevant to the subject matter and have been developed and exposed to peer review and a thorough due-diligence process by experts in various fields.
- **Criteria established by laws and regulations**—While laws and regulations can provide the basis of criteria, care must be taken in their use. Frequently, wording is complex and carries a specific legal meaning. In many cases, it may be necessary to restate the requirements as assertions. Further, expressing an opinion on legislation is usually restricted to members of the legal profession.
- **Criteria established by enterprises that do not follow due process**—These include relevant criteria developed by other enterprises that did not follow due process and have not been subject to public consultation and debate.
- **Criteria developed specifically for the IS audit or assurance engagement**—While criteria developed specifically for the IS audit or assurance engagement may be appropriate, take particular care to ensure that these criteria meet the suitability criteria, particularly completeness, measurability and objectivity. Criteria developed specifically for an IS audit or assurance engagement are in the form of assertions.

The selection criteria should be considered carefully. While adhering to local laws and regulations is important and must be considered a mandatory requirement, it is recognised that many IS audit and assurance engagements include areas, such as change management, IT general controls and access controls, not covered by law or regulations. In addition, some industries, such as the payment card industry, have established mandatory requirements that must be met. Where legislative requirements are principle-based the professional should ensure that criteria selected meet the engagement objective.

As the engagement progresses, additional information may result in certain criteria not being necessary to achieve the objectives. In these circumstances, further work related to the criteria is not necessary.

Terms

Term	Definition
Criteria	The standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter. Criteria should be: • Objective—Free from bias • Complete—Include all relevant factors to reach a conclusion • Relevant—Relate to the subject matter • Measurable—Provide for consistent measurement • Understandable In an attestation engagement, benchmarks against which management's written assertion on the subject matter can be evaluated. The practitioner forms a conclusion concerning subject matter by referring to suitable criteria.

Linkage to Guidelines

Type	Title
Guideline	2008 Criteria

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

Performance Standards

Performance standards establish baseline expectations in the conduct of IS audit and assurance engagements. While these standards apply to IS audit assurance professionals performing any IS audit or assurance assignment, compliance is particularly important when they are acting in an audit capacity. Accordingly, the performance standards focus on the IS audit and assurance professional's attention to the design of the assurance work, the conduct of the assurance, the evidence required, and the development of IS audit and assurance findings and conclusions.

The performance standards are:
1201 Engagement Planning
1202 Risk Assessment in Planning
1203 Performance and Supervision
1204 Materiality
1205 Evidence
1206 Using the Work of Other Experts
1207 Irregularity and Illegal Acts

The standards are included here in their entirety. Underlined words are defined in the Terms section. For links to the individual standards, visit *www.isaca.org/standard*.

1201 Engagement Planning

Statements

1201.1 IS audit and assurance professionals shall plan each IS audit and assurance engagement to address:
- **Objective(s), scope, timeline and deliverables**
- **Compliance with applicable laws and professional auditing standards**
- **Use of a risk-based approach, where appropriate**
- **Engagement-specific issues**
- **Documentation and reporting requirements**

1201.2 IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the:
- **Engagement nature, objectives, timeline and resource requirements**
- **Timing and extent of audit procedures to complete the engagement**

Key Aspects

IS audit and assurance professionals should:
- Obtain an understanding of the activity being audited. The extent of the knowledge required should be determined by the nature of the enterprise, its environment, areas of risk, and the objectives of the engagement.
- Consider subject matter guidance or direction, as afforded through legislation, regulations, rules, directives and guidelines issued by government or industry.
- Perform a risk assessment to provide reasonable assurance that all material items will be adequately covered during the engagement. Audit strategies, materiality levels and resource requirements can then be developed.
- Develop the engagement project plan using appropriate project management methodologies to ensure that activities remain on track and within budget.
- Include in the plan assignment-specific issues, such as:
  - Availability of resources with appropriate knowledge, skills and experience
  - Identification of tools needed for gathering evidence, performing tests and preparing/summarising information for reporting
  - Assessment criteria to be used
  - Reporting requirements and distribution
- Document the IS audit or assurance engagement's project plan to clearly indicate the:
  - Objective(s), scope and timing
  - Resources
  - Roles and responsibilities
  - Areas of risk identified and their impact on the engagement plan
  - Tools and techniques to be employed
  - Fact-finding interviews to be conducted
  - Relevant information to be obtained
  - Procedures to verify or validate the information obtained and its use as evidence
  - Assumptions regarding the approach, methodology, procedures, and anticipated results and conclusions
- Schedule the engagement with regard to the timing, availability, and other commitments and requirements of management and the auditee, to the extent possible.
- Adjust the project plan during the course of the IS audit or assurance engagement to address issues that arise during the engagement, such as new risk, incorrect assumptions or findings from the procedures already performed
- For internal engagements:
  - Communicate the audit charter to the auditee; where necessary use an engagement letter or equivalent to further clarify or confirm involvement in specific engagements.
  - Communicate the plan to the auditee so that the auditee is fully informed and can provide appropriate access to individuals, documents and other resources when required.
- For external engagements:
  - Prepare a separate engagement letter for each external IS audit and assurance engagement.
  - Prepare a project plan for each external IS audit and assurance engagement. The plan should, at a minimum, document the objective(s) and scope of the engagement.

1201 Engagement Planning *(cont.)*

Linkage to Guidelines

Type	Title
Guideline	2201 Engagement Planning

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1202 Risk Assessment in Planning

Statements

1202.1 The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources.

1202.2 IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements.

1202.3 IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.

Key Aspects

When planning ongoing activities, the IS audit and assurance function should:

- Conduct and document, at least annually, a risk assessment to facilitate the development of the IS audit plan.
- Include, as part of the risk assessment, the organisational strategic plans and objectives and the enterprise risk management framework and initiatives.
- For each IS audit and assurance engagement, quantify and justify the amount of IS audit resources needed to meet the engagement requirements.
- Use risk assessments in the selection of areas and items of audit interest and the decisions to design and conduct particular IS audit and assurance engagements.
- Seek approval of the risk assessment from the audit stakeholders and other appropriate parties.
- Prioritise and schedule IS audit and assurance work based on assessments of risk.
- Based on the risk assessment, develop a plan that:
  - Acts as a framework for IS audit and assurance activities
  - Considers non-IS audit and assurance requirements and activities
  - Is updated at least annually and approved by those charged with governance
  - Addresses responsibilities set by the audit charter

When planning an individual engagement, IS audit and assurance professionals should:

- Identify and assess risk relevant to the area under review.
- Conduct a preliminary assessment of the risk relevant to the area under review for each engagement. Objectives for each specific engagement should reflect the results of the preliminary risk assessment.
- In considering risk areas and planning a specific engagement, consider prior audits, reviews and findings, including any remedial activities. Also consider the board's overarching risk assessment process.
- Attempt to reduce audit risk to an acceptable level, and meet the audit objectives by an appropriate assessment of the IS subject matter and related controls, while planning and performing the IS audit.
- When planning a specific IS audit procedure, recognise that the lower the materiality threshold, the more precise the audit expectations and the greater the audit risk.
- To reduce risk for higher materiality, compensate by either extending the test of controls (reduce control risk) and/or extending the substantive testing procedures (reduce detection risk) to gain additional assurance.

Terms

Term	Definition
Audit charter	A document approved by those charges with governance that defines the purpose, authority and responsibility of the internal audit activity The charter should: • Establish the internal audit function's position within the enterprise • Authorise access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagements • Define the scope of audit function's activities

1202 Risk Assessment in Planning *(cont.)*

Terms (cont.)

Term	Definition
Audit risk	The risk of reaching an incorrect conclusion based upon audit findings. The three components of audit risk are: • Control risk • Detection risk • Inherent risk
Audit subject matter risk	Risk relevant to the area under review: • Business risk (customer capability to pay, credit worthiness, market factors, etc.) • Contract risk (liability, price, type, penalties, etc.) • Country risk (political, environment, security, etc.) • Project risk (resources, skill set, methodology, product stability, etc.) • Technology risk (solution, architecture, hardware and software infrastructure network, delivery channels, etc.) See inherent risk.
Control risk	The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal control. See inherent risk.
Detection risk	The risk that the IS audit or assurance professional's substantive procedures will not detect an error that could be material, individually or in combination with other errors. See audit risk.
Inherent risk	The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls). See control risk.
Materiality	An audit concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole.
Risk assessment	A process used to identify and evaluate risk and its potential effects Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan. Risk assessments are also used to manage the project delivery and project benefit risk.
Substantive testing	Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period

Linkage to Guidelines

Type	Title
Guideline	2202 Risk Assessment in Planning

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1203 Performance and Supervision

Statements

1203.1 IS audit and assurance professionals shall conduct the work in accordance with the approved IS audit plan to cover identified risk and within the agreed-on schedule.

1203.2 IS audit and assurance professionals shall provide supervision to IS audit staff for whom they have supervisory responsibility, to accomplish audit objectives and meet applicable professional audit standards.

1203.3 IS audit and assurance professionals shall accept only tasks that are within their knowledge and skills or for which they have a reasonable expectation of either acquiring the skills during the engagement or achieving the task under supervision.

1203.4 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to achieve the audit objectives. The audit findings and conclusions shall be supported by appropriate analysis and interpretation of this evidence.

1203.5 IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions.

1203.6 IS audit and assurance professionals shall identify and conclude on findings.

Key Aspects

IS audit and assurance professionals should:

- Assign team members to match their skills and experience with the engagement needs.
- Add external resources to the IS audit team, where appropriate and ensure that their work is properly supervised.
- Manage the roles and responsibilities of the specific IS audit team members throughout the engagement, addressing at a minimum:
  - Execution and review roles
  - Responsibility for designing the methodology and approach
  - Creating the audit or assurance programmes
  - Conducting the work
  - Dealing with issues, concerns and problems as they arise
  - Documenting and clearing the findings
  - Writing the report
- Have every task of the engagement executed by a team member(s) reviewed by another appropriate team member.
- Use the best audit evidence attainable, which is consistent with the importance of the audit objective and the time and effort involved in obtaining the evidence.
- Obtain additional evidence if, in the professional's judgement, the evidence obtained does not meet the criteria of being sufficient, and appropriate to form an opinion or support the findings and conclusions.
- Organise and document the work performed during the engagement following predefined documented and approved procedures.
- Include in documentation:
  - Audit objectives and scope of work, the audit programme, audit steps performed, evidence gathered, findings, conclusions and recommendations.
  - Detail sufficient to enable a prudent, informed person to re-perform the tasks performed during the engagement and reach the same conclusion.
  - Identification of who performed each task and their roles in preparing and reviewing the documentation.
  - The date the documentation was prepared and reviewed.
- Obtain relevant written representations from the auditee that clearly detail critical areas of the engagement, issues that have arisen and their resolution, and assertions made by the auditee.
- Determine that auditee representations have been signed and dated by the auditee to indicate acknowledgement of their responsibilities with respect to the engagement.
- Document and retain in work-papers any representations received during the course of conducting the engagement, either written or oral.

1203 Performance and Supervision *(cont.)*

Linkage to Standards and Guidelines

Type	Title
Standard	1005 Due Professional Care
Standard	1205 Evidence
Standard	1401 Reporting
Guideline	2202 Risk Assessment in Planning

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1204 Materiality

Statements

1204.1 IS audit and assurance professionals shall consider potential weaknesses or absences of controls while planning an engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness.

1204.2 IS audit and assurance professionals shall consider materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures.

1204.3 IS audit and assurance professionals shall consider the cumulative effect of minor control deficiencies or weaknesses and whether the absence of controls translates into a significant deficiency or a material weakness.

1204.4 IS audit and assurance professionals shall disclose the following in the report:
- **Absence of controls or ineffective controls**
- **Significance of the control deficiencies**
- **Probability of these weaknesses resulting in a significant deficiency or material weakness**

Key Aspects

In performing an engagement, IS audit and assurance professionals should:
- Apply the concept of materiality in:
  – Planning and performing the engagement
  – Evaluating the effect of specific items, processes, controls or errors

  Any deficiency, weakness or lack of appropriate policies, procedures and controls should be judged in the particular circumstances of the engagement.
- Consider definitions of materiality where provided by legislative or regulatory authorities.
- Note that the assessment of materiality and audit risk may vary from time to time, depending upon the circumstances and the changing environment.
- Attempt to reduce audit risk to an acceptable level and meet the objectives while planning and performing the engagement.
- Consider materiality when determining the nature, timing and extent of audit procedures.
- Reduce audit risk for higher materiality subject areas by either extending the test of controls (reduce control risk) and/or extending the substantive testing procedures (reduce detection risk).
- Evaluate the effect of compensating controls and whether such compensating controls are effective in determining whether a control deficiency or combination of control deficiencies is a material weakness.
- Consider the cumulative effect of multiple errors or control failures when determining materiality.
- Consider not only the size but also the nature of control deficiencies, and the particular circumstances of their occurrence, when evaluating their overall effect on the audit opinion or conclusion.

Terms

Term	Definition
Audit risk	The risk of reaching an incorrect conclusion based upon audit findings. The three components of audit risk are: • Control risk • Detection risk • Inherent risk
Material weakness	A deficiency or a combination of deficiencies in internal control, such that there is a reasonable possibility that a material misstatement will not be prevented or detected on a timely basis. Weakness in control is considered material if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. A weakness classified as material implies that: • Controls are not in place and/or controls are not in use and/or controls are inadequate • Escalation is warranted There is an inverse relationship between materiality and the level of audit risk acceptable to the IS audit or assurance professional, i.e., the higher the materiality level, the lower the acceptability of the audit risk, and *vice versa.*

1204 Materiality *(cont.)*

Terms (cont.)

Term	Definition
Materiality	An audit concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole.

Linkage to Standards and Guidelines

Type	Title
Standard	1201 Engagement Planning
Standard	1202 Risk Assessment in Planning
Standard	1207 Irregularity and Illegal Acts
Standard	1401 Reporting
Guideline	2202 Risk Assessment in Planning
Guideline	2204 Materiality

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1205 Evidence

Statements

1205.1 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results.

1205.2 IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

Key Aspects

In performing an engagement, IS audit and assurance professionals should:

- Obtain sufficient and appropriate evidence, including:
  - The procedures as performed
  - The results of procedures performed
  - Source documents (in either electronic or paper format), records and corroborating information used to support the engagement
  - Findings and results of the engagement
  - Documentation that the work was performed and complies with applicable laws, regulations and policies
- Prepare documentation, which should be:
  - Retained and available for a time period and in a format that complies with the audit or assurance organisation's policies and relevant professional standards, laws and regulations.
  - Protected from unauthorised disclosure or modification throughout its preparation and retention.
  - Properly disposed of at the end of the retention period.
- Consider the sufficiency of the evidence to support the assessed level of control risk when obtaining evidence from a test of controls.
- Appropriately identify, cross-reference and catalogue evidence.
- Consider properties such as the source, nature (e.g., written, oral, visual, electronic) and authenticity (e.g., digital and manual signatures, stamps) of the evidence when evaluating its reliability.
- Consider the most cost-effective and timely means of gathering the necessary evidence to satisfy the objectives and risk of the engagement. However, difficulty or cost is not a valid basis for omitting a necessary procedure.
- Select the most appropriate procedure to gather evidence depending on the subject matter being audited (i.e., its nature, timing of the audit, professional judgement). Procedures used to obtain the evidence include:
  - Inquiry and confirmation
  - Reperformance
  - Recalculation
  - Computation
  - Analytical procedures
  - Inspection
  - Observation
  - Other generally accepted methods
- Consider the source and nature of any information obtained to evaluate its reliability and further verification requirements. In general terms, evidence reliability is greater when it is:
  - In written form, rather than oral expressions
  - Obtained from independent sources
  - Obtained by the professional rather than by the entity being audited
  - Certified by an independent party
  - Kept by an independent party
  - The result of inspection
  - The result of observation
- Obtain objective evidence that is sufficient to enable a qualified independent party to reperform the tests and obtain the same results and conclusions.
- Obtain evidence commensurate with the materiality of the item and the risk involved.
- Place due emphasis on the accuracy and completeness of the information when information obtained from the enterprise is used by the IS audit or assurance professional to perform audit procedures.
- Disclose any situation where sufficient evidence cannot be obtained in a manner consistent with the communication of the IS audit or assurance engagement results.
- Secure evidence against unauthorised access and modification.
- Retain evidence after completion of the IS audit or assurance work as long as necessary to comply with all applicable laws, regulations and policies.

1205 Evidence *(cont.)*

Terms

Term	Definition
Appropriate evidence	The measure of the quality of the evidence
Sufficient evidence	The measure of the quantity of evidence; supports all material questions to the audit objective and scope. See evidence.

Linkage to Standards and Guidelines

Type	Title
Guideline	2205 Evidence

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1206 Using the Work of Other Experts

Statements

1206.1 IS audit and assurance professionals shall consider using the work of other experts for the engagement, where appropriate.

1206.2 IS audit and assurance professionals shall assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.

1206.3 IS audit and assurance professionals shall assess, review and evaluate the work of other experts as part of the engagement, and document the conclusion on the extent of use and reliance on their work.

1206.4 IS audit and assurance professionals shall determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives, and clearly document the conclusion.

1206.5 IS audit and assurance professionals shall determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.

1206.6 IS audit and assurance professionals shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.

1206.7 IS audit and assurance professionals shall provide an appropriate audit opinion or conclusion, and include any scope limitation where required evidence is not obtained through additional test procedures.

Key Aspects

IS audit and assurance professionals should:

- Consider using the work of other experts in the engagement when there are constraints (e.g., technical knowledge required by the nature of the tasks to be performed, scarce audit resources, time constraints) that could impair the work to be performed or potential gains in the quality of the engagement.
- Document the impact on achieving the engagement objectives if required experts cannot be obtained and insert specific tasks in the engagement plan to manage risk and evidence requirements.
- Consider independence of other experts when using their work.
- Have access to all work papers, supporting documentation and reports of other experts, where such access does not create legal issues.
- Determine and conclude on the extent of use and reliance on the expert's work where the expert is not granted access to records due to legal issues.
- Document the use of the other expert's work in the report.

Terms

Term	Definition
Other expert	Internal or external to an enterprise, other expert could refer to: • An IS auditor from the external accounting firm • A management consultant • An expert in the area of the engagement who has been appointed by top management or by the team

Linkage to Standards and Guidelines

Type	Title
Guideline	2206 Using the Work of Other Experts

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1207 Irregularity and Illegal Acts

Statements

1207.1 IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement.

1207.2 IS audit and assurance professionals shall maintain an attitude of professional scepticism during the engagement.

1207.3 IS audit and assurance professionals shall document and communicate any material irregularities or illegal act to the appropriate party in a timely manner.

Key Aspects

IS audit and assurance professionals should:

- Reduce audit risk to an acceptable level in planning and performing the engagement by :
  - Being aware that material errors, control deficiencies or misstatements due to irregularities and illegal acts could exist, irrespective of evaluation of the risk of irregularities and illegal acts
  - Obtaining an understanding of the enterprise and its environment, including internal controls intended to prevent or detect irregularities and illegal acts that are relevant to the engagement subject matter, scope and objectives
  - Obtaining sufficient and appropriate evidence to determine whether management or others within the enterprise have knowledge of any actual, suspected or alleged irregularities and illegal acts
- Consider unusual or unexpected relationships that may indicate a risk of material errors, control deficiencies or misstatements due to irregularities and illegal acts when performing audit procedures.
- Design and perform procedures to test the appropriateness of internal control and the risk that management overrides controls intended to prevent or detect irregularities and illegal acts.
- Assess whether identified errors, control deficiencies or misstatements may be indicative of an irregularity or illegal act. If there is such an indication, consider the implications in relation to other aspects of the engagement and, in particular, the representations of management.
- Obtain written representations from management at least annually or more often depending on the engagement to:
  - Acknowledge management's responsibility for the design and implementation of internal controls to prevent and detect irregularities and illegal acts.
  - Disclose the pertinent results of any risk assessment that indicates errors, control deficiencies or misstatements may exist as a result of an irregularity or illegal act.
  - Disclose management's knowledge of irregularities and illegal acts affecting the enterprise in relation to management and employees who have significant roles in internal control.
  - Disclose management's knowledge of any alleged or suspected irregularities and illegal acts affecting the enterprise as communicated by employees, former employees, regulators and others.
- Communicate in a timely manner to:
  - The appropriate level of management any information identified or obtained that a material irregularity or illegal act may exist.
  - Those charged with governance, any material irregularity and illegal acts involving management or employees who have significant roles in internal control.
- Report to those charged with governance any material weakness in the design and implementation of internal controls intended to prevent and detect any irregularities and illegal acts that are identified during the engagement, even if they are outside of the scope.
- Consider the legal and professional reporting requirements applicable in the circumstances.
- Consider withdrawing from the engagement if material errors, control deficiencies, misstatements or illegal acts affect the continued performance of the engagement.
- Document all communications, planning, results, evaluations and conclusions relating to material irregularities and illegal acts that have been reported to management, those charged with governance, regulators and others.

1207 Irregularity and Illegal Acts *(cont.)*

Terms

Term	Definition
Irregularity	Violation of an established management policy or regulatory requirement. It may consist of deliberate misstatements or omission of information concerning the area under audit or the enterprise as a whole gross negligence or unintentional illegal acts.
Material misstatement	An accidental or intentional untrue statement that affects the results of an audit to a measurable extent
Professional scepticism	An attitude that includes a questioning mind and a critical assessment of audit evidence. Source: American Institute of Certified Public Accountants (AICPA) AU 230.07

Linkage to Standards and Guidelines

Type	Title
Standard	1008 Criteria
Standard	1202 Risk Assessment in Planning
Standard	1205 Evidence
Guideline	2206 Using the Work of Other Experts
Guideline	2207 Irregularity and Illegal Acts

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

Reporting Standards

The reports produced by IS audit and assurance professionals will vary, depending on the type of assignments performed. Considerations include the levels of assurance, whether IS audit and assurance professionals were acting in an audit capacity, whether they are providing direct reports on the subject matter or reporting on assertions regarding the subject matter, and whether the reports are based on work performed at the review level or the examination level.

The reporting standards are:
1401 Reporting
1402 Follow-up Activities

The standards are included here in their entirety. Underlined words are defined in the Terms section. For links to the individual standards, visit *www.isaca.org/standard*.

1401 Reporting

Statements

1401.1 IS audit and assurance professionals shall provide a report to communicate the results upon completion of the engagement including:
- **Identification of the enterprise, the intended recipients and any restrictions on content and circulation**
- **The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed**
- **The findings, conclusions and recommendations**
- **Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement**
- **Signature, date and distribution according to the terms of the audit charter or engagement letter**

1401.2 IS audit and assurance professionals shall ensure that findings in the audit report are supported by sufficient and appropriate evidence.

Key Aspects

IS audit and assurance professionals should:
- Obtain relevant written representations from the auditee that clearly detail critical areas of the engagement, issues that have arisen and their resolution, and assertions made by the auditee.
- Determine that auditee representations have been signed and dated by the auditee to indicate acknowledgement of auditee responsibilities with respect to the engagement.
- Document and retain in the work paper any representations, either written or oral, received during the course of conducting the engagement. For attestation engagements, representations from the auditee should be obtained in writing to reduce possible misunderstanding.
- Customise the form and content of the report to support the type of the engagement performed, such as:
  – Audit (direct or attest)
  –Review (direct or attest)
  –Agreed-upon procedures
- Describe material or significant weaknesses and their effect on the achievement of the engagement objectives in the report.
- Discuss the draft report contents with management in the subject area prior to finalisation and release, and include management's response to findings, conclusions and recommendations in the final report, where applicable.
- Communicate significant deficiencies and material weaknesses in the control environment to those charged with governance and, where applicable, to the responsible authority. Disclose in the report that these have been communicated.
- Reference any separate reports in the final report.
- Communicate to auditee management internal control deficiencies that are less than significant but more than inconsequential. In such cases, those charged with governance or the responsible authority should be notified that such internal control deficiencies have been communicated to auditee management.
- Identify standards applied in conducting the engagement. Communicate any non-compliance with these standards, as applicable.

1401 Reporting *(cont.)*

Terms

Term	Definition
Relevant information	Relating to controls, tells the evaluator something meaningful about the operation of the underlying controls or control component. Information that directly confirms the operation of controls is most relevant. Information that relates indirectly to the operation of controls can also be relevant, but is less relevant than direct information. Refer to COBIT 5 information quality goals
Reliable information	Information that is accurate, verifiable and from an objective source. Refer to COBIT 5 information quality goals
Sufficient information	Information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. For information to be sufficient, however, it must first be suitable. Refer to COBIT 5 information quality goals
Suitable information	Relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source) and timely (i.e., produced and used in an appropriate time frame) information. Refer to COBIT 5 information quality goals
Timely information	Produced and used in a time frame that makes it possible to prevent or detect control deficiencies before they become material to an enterprise. Refer to COBIT 5 information quality goals

Linkage to Standards and Guidelines

Type	Title
Guideline	2401 Reporting

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

1402 Follow-up Activities

Statements

1402.1 IS audit and assurance professionals shall monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations.

Key Aspects

The internal IS audit function should 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.

External IS audit or assurance professionals may rely on an internal IS audit function to follow up on their agreed-on recommendations, depending on the scope and terms of the engagement.

Linkage to Standards and Guidelines

Type	Title
Guideline	2402 Follow-up Activities

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

2. IS Audit and Assurance Guidelines

Section 2000 addresses guidelines to support the standards:
2000 General Guidelines
2200 Performance Guidelines
2400 Reporting Guidelines

Each section within the guidelines focuses on one of the following:
- IS issues and processes that the IS audit and assurance professional should understand and consider when determining the planning, scoping, execution and reporting of IS audit or assurance activities
- IS audit and assurance processes, procedures, methodologies and approaches that the IS audit and assurance professional should consider when conducting IS audit or assurance activities

Note that these guidelines are in the process of being updated for the new standards and COBIT 5. Please watch the ISACA web site for exposure drafts scheduled to be issued by the end of 2013.

General Guidelines

The general guidelines are:
2001 Audit Charter (G5)
2002 Organisational Independence (G12)
2003 Professional Independence (G17)
2004 Reasonable Expectation (in development)
2005 Due Professional Care (G7)
2006 Proficiency (G30)
2007 Assertions (in development)
2008 Criteria (in development)

The guidelines are included here in their entirety. For links to the individual standards, visit *www.isaca.org/standard*.

2001 Audit Charter (G5)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S1 (1001) Audit Charter states 'The responsibility, authority and accountability of the information systems audit function or information audit assignments should be appropriately documented in an audit charter or engagement letter'.

1.2 Linkage to COBIT

1.2.1 ME 4.7 *Independent assurance* states '…Provide the board with timely independent assurance about the compliance of IT with its policies, standards and procedures, as well as with generally accepted practices'.

1.2.2 ME 2.5 *Assurance of internal control* states 'Obtain, as needed, further assurance of the completeness and effectiveness on internal controls through third-party reviews'.

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to assist the IS auditor to prepare an audit charter to define the responsibility, authority and accountability of the IS audit function. This guideline is aimed primarily at the internal IS audit function; however, aspects could be considered for other circumstances.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

2. Audit Charter

2.1 Mandate

2.1.1 The IS auditor should have a clear mandate to perform the IS audit function. This mandate is ordinarily documented in an audit charter that should be formally accepted. Where an audit charter exists for the audit function as a whole, the IS audit mandate should be incorporated.

2.2 Contents of the Audit Charter

2.2.1 The audit charter should clearly address the four aspects of purpose, responsibility, authority and accountability. Aspects to consider are set out in the following sections.

2.2.2 Purpose:

- Role
- Aims/goals
- Mission statement
- Scope
- Objectives

2.2.3 Responsibility:

- Operating principles
- Independence
- Relationship with external audit
- Auditee requirements
- Critical success factors
- Key performance indicators
- Risk assessment
- Other measures of performance

2.2.4 Authority:

- Right of access to information, personnel, locations and systems relevant to the performance of audits
- Scope or any limitations of scope
- Functions to be audited
- Auditee expectations
- Organisational structure, including reporting lines to board and senior management
- Grading of IS audit staff

2.2.5 Accountability:

- Reporting lines to senior management
- Assignment performance appraisals
- Personnel performance appraisals
- Staffing/career development
- Auditee rights
- Independent quality reviews
- Assessment of compliance with standards
- Benchmarking performance and functions

- Assessment of completion of the audit plan
- Comparison of budget to actual costs
- Agreed actions, e.g., penalties when either party fails to carry out their responsibilities

2.3 Communication With Auditees

2.3.1 Effective communication with auditees involves:

- Describing the service, its scope, its availability and timeliness of delivery
- Providing cost estimates or budgets if they are available
- Describing problems and possible resolutions for them
- Providing adequate and readily accessible facilities for effective communication
- Determining the relationship between the service offered and the needs of the auditee

2.3.2 The audit charter forms a sound basis for communication with auditees and should include references to service level agreements for such things as:

- Availability for unplanned work
- Delivery of reports
- Costs
- Response to auditee complaints
- Quality of service
- Review of performance
- Communication with auditees
- Needs assessment
- Control risk self-assessment
- Agreement of terms of reference for audits
- Reporting process
- Agreement of findings

2.4 Quality Assurance Process

2.4.1 The IS auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) to understand auditees' needs and expectations relevant to the IS audit function. These needs should be evaluated against the charter with a view to improving the service or changing the service delivery or audit charter, as necessary.

3. Engagement Letter

3.1 Purpose

3.1.1 Engagement letters are often used for individual assignments or for setting the scope and objectives of a relationship between external IS audit and an organisation.

3.2 Content

3.2.1 The engagement letter should clearly address the three aspects of responsibility, authority and accountability. Aspects to consider are set out in the following paragraphs.

3.2.2 Responsibility:

- Scope
- Objectives
- Independence
- Risk assessment
- Specific auditee requirements
- Deliverables

3.2.3 Authority:

- Right of access to information, personnel, locations and systems relevant to the performance of the assignment
- Scope or any limitations of scope
- Evidence of agreement to the terms and conditions of the engagement

3.2.4 Accountability:

- Intended recipients of reports
- Auditee rights
- Quality reviews
- Agreed completion dates
- Agreed budgets/fees if available

4. Effective Date

4.1 This guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 February 2008.

2002 Organisational Independence (G12)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S2 (1002, 1003) Independence states: 'In all matters related to the audit, the IS auditor should be independent of the auditee in both attitude and appearance'.

1.1.2 Standard S2 (1002, 1003) Independence states: 'The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment'.

1.1.3 Standard S3 (1005) Professional Ethics and Standards states: 'The IS auditor should adhere to the ISACA Code of Professional Ethics'.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the independence requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary.

1.2.2 PO4 *Define the IT processes, organisation and relationships* satisfies the business requirement for IT of being agile in responding to the business strategy whilst complying with governance requirements and providing defined and competent points of contact by focusing on establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes.

1.2.3 Secondary references:

- ME2 *Monitor and evaluate internal control*
- ME4 *Provide IT governance*

1.2.4 The information criteria most relevant are:

- Primary: Effectiveness and efficiency
- Secondary: Confidentiality, integrity, availability, compliance and reliability

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to expand on the meaning of 'independence' as used in standard S2 (1002, 1003) and to address the IS auditor's attitude and independence in IS auditing.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

2. Independence

2.1 Attitude

2.1.1 IS auditors should seek adherence to applicable codes of professional ethics and auditing standards in all of their work.

2.1.2 As per COBIT, the audit charter should ensure that the independence, authority and accountability of the audit function are maintained and established by appropriate members of the organisation's management team.

3. Planning

3.1 Staffing

3.1.1 The IS auditor establishes many relationships with people involved in the audit activity and has the opportunity to explore the innermost aspects of the area being audited, often the whole organisation. The IS auditor's attitude should always be appropriate to this role. Planning should take into account any known relationships.

3.1.2 IS auditors should not participate in an audit if their independence is impaired. For example, independence is impaired if IS auditors have some expectation of financial gain or other personal advantage due to their influence on the results of the audit. However, the IS auditors' independence would not necessarily be impaired as a result of performing an audit of IS where their personal transactions occur in the normal course of business.

3.1.3 At the beginning of the audit, IS auditors may be required to sign a conflict-of-interest statement to declare their independence.

3.2 Prioritised Audit Plan

3.2.1 COBIT process ME4 states: 'Management should provide for independent audit'. To achieve this objective, an audit plan should be established. This plan should verify that regular and independent assurance is obtained regarding the effectiveness, efficiency and economy of security and internal control procedures. Within this plan, management should determine priorities regarding obtaining independent assurance.

4. Performance of Audit Work

4.1 Organisation

4.1.1 IS auditors should be organisationally independent of the area being audited. Independence is impaired if the IS auditors have direct control over the area being audited. The IS auditors' independence can also be impaired if the IS auditors have direct reporting responsibility to those individuals who have direct control over the area being audited. The IS auditors' independence also may be impaired if IS auditors are required, for tracking purposes, to report their time expended in performing the audit, including progress, audit issues, etc., to the IT group responsible for those controls tested and who report the results to senior or executive management. This could be perceived as the IT group project managing the IS auditors and, thus, an impairment of the IS auditors' independence. In addition, IS auditors should take into consideration if independence has been impaired in situations where the scope of work performed is based on requirements of the control process owners for business or regulatory purposes.

4.1.2 Independence should be regularly assessed by the IS auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. IS auditors should consider the use of control self-assessment techniques in this continuous assessment process.

4.1.3 Depending on the assignment, IS auditors can interview persons, analyse organisational processes, gain assistance from the organisation's staff, etc. An IS auditor's attitude and appearance of independence should always be adequate to meet these situations. IS auditors should be aware that the appearance of independence can be influenced by their actions or associations. Perceptions of the IS auditors' independence could affect the acceptance of their work.

4.1.4 If IS auditors become aware that a situation or relationship is perceived to impair their independence, they should inform audit management of the perceived impairment as soon as possible.

4.2 Gathering Information

4.2.1 Amongst the various items needed to obtain an understanding of the organisation being audited, IS auditors, to preserve their independence, should review:

- Organisation policies and procedures relating to the independent assurance process
- Audit charter, mission statement, policies, procedures and standards, prior reports, and audit plans
- The organisational chart

4.3 Controls Evaluation

4.3.1 IS audit plans should define the activities from which IS auditors are required to be independent. IS auditors' independence from these activities should be regularly monitored by senior management, or by the person who determines and approves IS audit plans. This monitoring should include an assessment of the process for assigning individual IS auditors to specific assignments, to verify that this process assures independence and sufficient skills.

4.3.2 Verification of the IS auditors' adherence to applicable professional codes of conduct should always be carried out. In many circumstances, this should be sufficient to provide audit evidence of independence. If there is an indication that an IS auditor's independence has been compromised, a revision of the audit plan should be considered.

5. Reporting

5.1 Effect on Reporting

5.1.1 In circumstances where the IS auditor's independence is impaired and the IS auditor continues to be associated with the audit, the facts surrounding the issue of the IS auditor's independence should be disclosed to the appropriate management and in the report.

6. Effective Date

6.1 This guideline is effective for all IS audits beginning on or after 1 September 2000. The guideline has been reviewed and updated effective 1 August 2008.

2003 Professional Independence (G17)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S2 (1002, 1003) Independence states that in all matters related to the audit, the IT audit and assurance professional should be independent of the auditee in both attitude and appearance.

1.1.2 Standard S2 (1002, 1003) Independence states that the IT audit and assurance function should be sufficiently independent of the area or activity being reviewed to permit objective completion of the audit and assurance assignment.

1.1.3 Standard S3 (1005) Professional Ethics and Standards states that the IT audit and assurance professional should exercise due professional care, including observance of applicable professional standards in conducting audit and assurance assignments.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit and assurance assignment is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the effect of non-audit roles on the IT audit and assurance professional's independence, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 Primary IT processes are:

- PO6 *Communicate management aims and direction*
- PO9 *Assess and manage IT risks*
- PO10 *Manage projects*
- DS2 *Manage third-party services*
- DS7 *Educate and train users*
- ME2 *Monitor and evaluate internal controls*
- ME3 *Ensure regulatory compliance*
- ME4 *Provide IT governance*

1.2.3 Secondary IT processes are:

- PO7 *Manage IT human resources*
- DS10 *Manage problems*

1.2.4 The information criteria most relevant are:

- Primary: Reliability, confidentiality, compliance and efficiency
- Secondary: Effectiveness, integrity and availability

1.3 Need for Guideline

1.3.1 In many enterprises, the expectation of management, IT staff and internal audit is that IT audit and assurance professionals may be involved in non-audit activities such as:

- Defining information systems (IS) strategies relating to areas such as technology, applications and resources
- Evaluation, selection and implementation of technologies
- Evaluation, selection, customisation and implementation of third-party IS applications and solutions
- Design, development and implementation of custom-built IS applications and solutions
- Establishing good practices, policies and procedures relating to various IT functions
- Design, development, testing and implementation of security and control
- Managing IT projects

1.3.2 The non-audit role, in general, involves participation in the IT initiatives and IT project teams in working and/or advisory/consultative capacities on a full-time or part-time basis. IT audit and assurance professionals may fulfil a non-audit role involved in activities such as:

- The full-time temporary assignment or loan of IT audit and assurance staff to the IS project team
- The part-time assignment of an IT audit and assurance staff member as a member of the various project structures, such as the project steering group, project working group, evaluation team, negotiation and contracting team, implementation team, quality assurance team, and trouble shooting team
- Acting as an independent advisor or reviewer on an ad hoc basis

1.3.3 Such non-audit roles are an important part of the IT audit and assurance professional's contribution to the education and training of other members of the enterprise. They enable IT audit and assurance professionals to use their expertise and their knowledge of the enterprise to provide a unique and valuable contribution to the efficiency and effectiveness of the enterprise's IT investments. They also provide opportunities to raise the profile of the IT audit and assurance function and to give IT audit and assurance staff valuable practical experience.

1.3.4 Where the IT audit and assurance professional has been involved in a non-audit role in an IS initiative and an audit of that initiative or the related IS function is subsequently/concurrently performed, recommendations and conclusions arising from the audit may be perceived by the recipients as not objective. In this situation, the perception may be that both the independence and the objectivity of the IT audit and assurance professional have been impaired by non-audit involvement.

1.3.5 The IT audit and assurance professional involved in a non-audit role should evaluate whether this role generates an impairment of independence either in fact or appearance. The IT audit and assurance professional should advise and raise awareness of the IT decision maker on what to consider when evaluating if a control is adequate. The IT audit and assurance professional performing a non-audit role should not sign off on whether a control is designed effectively.

1.3.6 The purpose of this guideline is to provide a framework to enable the IT audit and assurance professional to:

- Establish when the required independence may be, or may appear to be, impaired
- Consider potential alternative approaches to the audit process when the required independence is, or may appear to be, impaired
- Reduce or eliminate the impact of IT audit and assurance professionals on non-audit roles, functions and services
- Determine the disclosure requirements

2. Audit Charter

2.1 Terms of Non-audit Involvement of IT Audit and Assurance Professionals

2.1.1 The IT audit charter should establish the mandate for the IT audit and assurance professional to be involved in non-audit roles and the broad nature, timing and extent of such roles, to ensure that independence is not impaired with respect to the systems the IT audit and assurance professional may audit. This would avoid the need to obtain specific mandates on a case-by-case basis.

2.1.2 The IT audit and assurance professional should provide reasonable assurance that the terms of reference (TOR) of specific non-audit roles are in conformity with the audit charter. Where there are any deviations, the same should be expressly spelled out in the TOR.

2.1.3 Where the audit charter does not specify the non-audit roles, or where there is no audit charter, IT audit and assurance professionals should report to management and the audit committee, if one exists, the fact of their involvement in non-audit roles. The timing or extent of IT audit and assurance professionals' involvement in IS projects should be subject to individual TOR signed by the function head and approved by the audit committee.

3 Types of Non-Audit Services

3.1. Involvements That Do Not Impair Independence

3.1.1 IT audit and assurance professionals providing technical advice based on their technical knowledge and expertise such as participating in commissions, committees, task forces or panels are non-audit involvements that do not impair the IT audit and assurance professionals' independence. However, audit and assurance professionals' independence would be impaired if the extent or nature of the advice resulted in the IT audit and assurance professionals making management decisions or performing management functions.

3.1.2 Non-audit involvements that would not impair independence if supplemental countermeasures are implemented include providing advice on information technology, limited to advising on system design, system installation and system security. The enterprise's board of directors and management, should rely on the IT audit and assurance professionals' work as the primary basis for determining whether to implement a new system, the adequacy of the new system design, the adequacy of major design changes to an existing system, and the adequacy of the system to comply with regulatory or other requirements.

3.2 Involvements That Do Impair Independence

3.2.1 Non-audit roles that impair independence and objectivity include material involvement of the IT audit and assurance professional in the processes of designing, developing, testing, installing, configuring or operating the information systems as well as designing controls for information systems that are material or significant to the subject matter of the audit.

3.2.2 Non-audit roles include serving in a governance role where the IT audit and assurance professional is responsible for either independently or jointly making management decisions or approving policies and standards.

3.2.3 IT audit and assurance professional independence could be impaired when evaluation of information systems implies testing controls of the applications/systems selected by the IT audit and assurance professional while performing a non-audit role.

3.2.4 IT audit and assurance professional independence could be impaired if the extent or nature of the advice resulted in the IT audit and assurance professional making management decisions or performing management functions.

4. Independence

4.1 Relevance of Independence in Non-audit Roles

4.1.1 IT audit and assurance professionals should be independent in all matters related to the audit, unless prohibited by other external standards, there is no requirement for the IT audit and assurance professional either to be, or to be seen to be, independent where the nature of the involvement in the IS initiative is one of a non-audit role.

4.1.2 Although there is no need for the IT audit and assurance professional to be independent when carrying out tasks relating to a non-audit role, objectivity is still a professional requirement. The IT audit and assurance professional should carry out the tasks relating to the non-audit role in an objective and professional manner.

4.1.3 Despite there being no requirement for the IT audit and assurance professional to be independent while playing a non-audit role in an IS initiative, the IT audit and assurance professional should consider whether such a role could be deemed to impair independence if the IT audit and assurance professional is assigned to audit the IS initiative and/or the related function. Where such a conflict is foreseeable (e.g., where an independent audit will be required later and there is only one IT audit and assurance professional with the requisite skills to carry out both the non-audit role and the subsequent audit), the IT audit and assurance professional should discuss the issue with the audit committee or equivalent governance body prior to embarking on the non-audit role.

4.1.4 Determining the participation of the IT audit and assurance professional in a non-audit role in an IS initiative and the independent audit of the IS initiative or the related function should be the decision of the audit committee or equivalent governance body. A risk analysis should be performed. Aspects that are likely to influence the decision include:

- Potential alternative resources for either role
- The perception of relative value added by the conflicting activities
- Potential for educating the IS team so that future initiatives could benefit
- Career development opportunities and succession planning for the IT audit and assurance professional
- Level of risk attached to a non-audit role
- Effect on the visibility, profile, image, etc., of the IT audit and assurance function
- Effect of the decision on the requirements of external auditors or regulators, if any
- The provisions of the IT audit charter

4.2 Effect of Non-audit Roles on Subsequent Audits

4.2.1 When an IS initiative or function is being audited as per statutory and/or management requirements, the IT audit and assurance professional should be, and be seen to be, independent of the IS team and its management.

4.2.2 IT audit and assurance professionals should not audit their own work or provide non-audit services in situations in which the non-audit works are significant or material to the subject matter of audits in which they are involved. IT audit and assurance professionals' non-audit involvement in an IS initiative could potentially impair their independence with reference to the audit of the IS initiative and/or the related function. IT audit and assurance professionals should state whether, in their opinion, their independence while carrying out the audit is or is not impaired by their non-audit role. The audit committee or equivalent governance body should be requested to concur with the opinion in writing.

4.2.3 The critical factors that could help determine whether the IT audit and assurance professionals' independence with reference to an audit could be impaired or not by a non-audit role include aspects such as the:

- Nature, timing and extent of the non-audit role in the IS initiative, when an audit of the IT initiative and/or its related function is being considered. The greater the decision powers of the non-audit role, the higher the level of impairment to independence.
- Existence of facts that may be perceived to undermine independence. This includes aspects such as material bonus or penalty relating to the non-audit role.
- Ability as well as the commitment of the IT audit and assurance professional to remain unbiased and impartial while conducting the audit and reporting the weaknesses or errors despite the nonaudit role
- Freedom of the IT audit and assurance professional to determine the scope and conduct of the audit despite involvement in a non-audit role
- Disclosure by the IT audit and assurance professional of the non-audit role, the level of involvement in that capacity and the material facts relating to it
- Existence of significant personal relationships (positive or negative) made while in the non-audit role, particularly with those in management positions
- Influence and/or persuasion of the IT audit and assurance professional in the non-audit role, regardless of the decision-making powers of the IT audit and assurance professional
- Criticality (risk rating priority) of information resources that are going to be subjects of audit and already have been subjects of the non-audit role performed by the same person

5. Planning

5.1 Effect on Independence

5.1.1 The potential effect of the non-audit role on independence with reference to the likely future/concurrent audit of the same IS initiative or related function should be evaluated while planning any non-audit roles.

5.1.2 The potential effect of any previous or ongoing non-audit roles of IT audit and assurance professionals in any IS initiative on their independence should be evaluated while planning the audits of any such IT initiatives and or related functions.

5.1.3 The audit committee or equivalent governance body should be informed about the potential impairment of independence as well as any potential appearance of such impairment.

5.1.4 The IT audit and assurance professional should recommend actions or compensating controls that could be taken by the audit management/committee to provide reasonable assurance of independence and objectivity. These could include:
- Assigning additional management and/or staff from within the IT audit and assurance function who did not have any non-audit role in the area being audited, to supplement the IT audit and assurance professional who has/had a non-audit role
- Assigning management and staff from outside the IT audit and assurance function, such as borrowing staff from another function, division, external organisation, etc., to supplement the IT audit and assurance professional who has/had a non-audit role
- Assigning an independent resource, from within the IT audit and assurance function or other sources referenced previously, to carry out a peer review and to act as an independent arbiter during planning, field work and reporting

5.1.5 When the extent of IT audit and assurance professionals' involvement in the non-audit role is very strong, IT audit and assurance professionals should not recommend actions to the audit committee nor should they be directly involved in the review of the subject audit area in which they were already fully involved/participated.

6. Performance of Audit Work

6.1. Monitoring the Conduct of Audit

6.1.1 In the case of an audit where there is potential for impaired independence due to non-audit involvement, IT audit and assurance management should closely monitor the conduct of the audit. Any material indications of the compromise of independence arising out of non-audit involvement should be evaluated critically by IT audit and assurance management and necessary corrective actions should be initiated. In such instances, the audit committee or equivalent governance body should be informed.

6.1.2 In considering whether audits performed by the IT audit and assurance professionals could be significantly or materially affected by the non-audit role, the audit committee or equivalent governance body should evaluate ongoing audits; planned audits; requirements and commitments for audits, which include laws, regulations, rules, contracts and other agreements; and policies or decisions that place responsibilities on the IT audit and assurance professionals due to their involvement in a non-audit role.

6.1.3 Governance bodies should include the allocation of audit resources to non-audit roles, so they can be made aware of potential conflicts in advance and receive assurance from audit management that such conflicts will be minimised and adequately managed.

7. Reporting

7.1 Disclosure Requirements

7.1.1 Where the independence of IT audit and assurance management and/or staff, with reference to an audit of an IS initiative and/or the related function, could be, or could appear to be, impaired by a non-audit role in the IS initiative, the IT audit and assurance professional should disclose in the audit report sufficient information about the non-audit role as well as the actions taken to provide reasonable assurance of independence and objectivity. This will enable the users of the audit report to understand the likely extent of the impairment, if any, and the measures taken to mitigate the effects of it. Information that IT audit and assurance professionals should consider disclosing includes aspects such as:
- Names and seniority of the IT audit and assurance management and staff involved in the IT initiative in non-audit roles
- Nature, timing and extent of their non-audit involvement in the IS initiative
- Reasons for their involvement in the non-audit role in the IS initiative as well as in the audit of the IS initiative or the related function
- Steps taken to provide assurance that independence and objectivity has not been materially impaired in the course of the audit work and the reporting process
- The fact that the potential impairment of independence has been highlighted to the audit committee or equivalent governance body and their agreement obtained before undertaking the non-audit role
- Existence and extent of the review undertaken to ensure the acceptable level of reliance on the work performed

8. Effective Date

8.1 This guideline has been reviewed and updated, and is effective for all IT audits beginning on or after 1 May 2010.

2004 Reasonable Expectation (in development)

2005 Due Professional Care (G7)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S3 (1005) Professional Ethics and Standards, states 'The IS auditor should adhere to the ISACA Code of Professional Ethics in conducting audit assignments'.

1.1.2 Standard S3 (1005) Professional Ethics and Standards, states 'The IS auditor should exercise due professional care, including observance of applicable professional auditing standards'.

1.1.3 Standard S2 (1002, 1003) Independence, states 'In all matters related to the audit, the IS auditor should be independent of the auditee in both attitude and appearance'.

1.1.4 Standard S4 (1006) Professional Competence, states 'The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment, and he/she should maintain professional competence through appropriate continuing professional education and training'.

1.1.5 The IS auditor should refer to the commentary sections in the above standards for additional guidance.

1.2 Linkage to COBIT

1.2.1 PO6 *Communicate management aims and direction*, satisfies the business requirement for IT of accurate and timely information on the current and future IT services, associated risks and responsibilities by focusing on providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders embedded in an IT control framework.

1.2.2 PO7 *Manage IT human resources*, satisfies the business requirement for IT of competent and motivated people to create and deliver IT services by focusing on hiring and training personnel, motivating through clear career paths, assigning roles that correspond with skills, establishing a defined review process, creating position descriptions and ensuring awareness of dependency on individuals.

1.2.3 PO9 *Assess and manage IT risks*, satisfies the business requirement for IT of analysing and communicating IT risks and their potential impact on business processes and goals by focusing on development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk.

1.2.4 ME3 *Ensure compliance with external requirements*, satisfies the business requirement for IT of ensuring compliance with laws regulations and contractual requirements by focusing on identifying all applicable laws regulations and contracts and the corresponding level of IT compliance and optimising IT processes to reduce the risk of non-compliance.

1.2.5 ME4 *Provide IT governance*, satisfies the business requirement for IT of integrating IT governance with corporate governance objectives and complying with laws, regulations and contracts by focusing on preparing board reports on IT strategy, performance and risks and responding to governance requirements in line with board directions.

1.2.6 Secondary references:

- PO1 *Define a strategic IT plan*
- PO5 *Manage the IT investment*
- PO8 *Manage quality*
- PO10 *Manage projects*
- AI1 *Identify automated solutions*
- AI6 *Manage changes*
- DS3 *Manage performance and capacity*
- DS7 *Educate and train users*
- DS9 *Manage configuration*
- DS10 *Manage problems*

1.2.7 The information criteria most relevant are:

- Primary: Reliability, confidentiality, integrity, compliance and efficiency
- Secondary: Effectiveness and availability

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to clarify the term 'due professional care' as it applies to the performance of an audit in compliance with standard S3 (1005) of the IS Auditing Standards.

1.3.2 Members and ISACA certification holders are expected to comply with the ISACA Code of Professional Ethics; failure may result in an investigation into the member/certification holder's conduct and ultimately in disciplinary action, if necessary.

1.3.3 The guideline provides guidance in applying IS Auditing Standards and complying with the ISACA Code of Professional Ethics on performance of duties with due diligence and professional care. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

2. Performance of Audit Work

2.1 Due Professional Care

2.1.1 The standard of due care is the level of diligence that a prudent and competent expert would exercise under a given set of circumstances. Due professional care applies to an individual who professes to exercise a special skill, such as IS auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by practitioners of that speciality.

2.1.2 Due professional care applies to the exercise of professional judgement in the conduct of work performed. Due professional care implies that the professional approaches matters requiring professional judgement with proper diligence.

2.1.3 Due professional care should extend to every aspect of the audit, including but not restricted to the evaluation of audit risk, accepting audit assignments, formulation of audit objectives, the establishment of the audit scope, planning the audit, conducting the audit, allocation of resources to the audit, selection of audit tests, evaluation of test results, audit documentation, conclusion of audit, reporting and delivery of audit results. In doing this, the IS auditor should determine or evaluate:

- The type, level, skill and competence of audit resources required to meet the audit objectives
- The significance of identified risks and the potential affect of such risks on the audit
- The audit evidence gathered
- The competence, integrity and conclusions of others upon whose work the IS auditor places reliance

2.1.4 The IS auditor should maintain an independent and objective state of mind in all matters related to the conduct of the IT audit assignment. The auditor should appear honest, impartial and unbiased in addressing audit issues and reaching conclusions.

2.1.5 The IS auditor should conduct the audit with diligence while adhering to professional standards and statutory and regulatory requirements. The IS auditor should have a reasonable expectation that the IS audit assignment can be completed in accordance with established IS audit standards and other appropriate professional, regulatory or industry standards, and will result in the IS audit being able to express a professional opinion. The IS auditor should disclose the circumstances of any noncompliance in a manner consistent with the communication of the audit results.

2.1.6 The IS auditor should have satisfactory assurance that management understands its obligations and responsibilities in providing appropriate, relevant and timely information required in the performance of the audit assignment and ensure the co-operation of relevant personnel during the audit.

2.1.7 The IS auditor should serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and should not engage in acts discreditable to the profession.

2.1.8 The IS auditor should maintain the privacy and confidentiality of information obtained in the course of his/her duties unless disclosure is required by legal authority. Such information should not be used for personal benefit or released to inappropriate parties.

2.1.9 The IS auditor should exercise due professional care while informing appropriate parties of the results of work performed.

2.1.10 The intended recipients of the audit reports have an appropriate expectation that the IS auditor has exercised due professional care throughout the course of the audit. The IS auditor should not accept an assignment unless adequate skills, knowledge and other resources are available to complete the work in a manner expected of a professional.

3. Effective Date

3.1 This guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 March 2008.

2006 Proficiency (G30)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S4 (1006) Professional Competence states, "The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment. The IS auditor should maintain professional competence through appropriate continuing professional education and training."

1.2 Linkage to COBIT

1.2.1 High-level control objective M3 (Obtain Independent Assurance) states, "…obtaining independent assurance to increase confidence and trust amongst the organisations, customers and third-party providers."

1.2.2 High-level control objective M4 (Provide for Independent Audit) states, "…providing for independent audit to increase confidence levels and benefit from best practice advice."

1.2.3 Detailed control objective M3.7 (Competence of Independent Assurance Function) states, "Management should ensure that the independent assurance function possesses the technical competence, skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner."

1.2.4 Detailed control objective M4.4 (Competence) states, "Management should ensure that the auditors responsible for the review of the organisation's IT activities are technically competent and collectively possess the skills and knowledge (i.e., CISA domains) necessary to perform such reviews in an effective, efficient and economical manner. Management should ensure that audit staff assigned to information systems auditing tasks maintain technical competence through appropriate continuing professional education".

1.3 COBIT Reference

1.3.1 The COBIT references offer the specific objectives or processes of COBIT to consider when reviewing the area addressed by this guidance. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the requirement, the processes in COBIT likely to be the most relevant are selected and adapted and are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- PO7—*Manage Human Resources*
- M2—*Assess Internal Control Adequacy*
- M3—*Obtain Independent Assurance*
- M4—*Provide for Independent Audit*

1.3.3 Secondary:

- DS1—*Define and Manage Service Levels*
- DS2—*Manage Third Party Services*
- DS3—*Manage Performance and Capacity*
- DS7—*Educate and Train Users*
- M1—*Monitor the Process*

1.3.4 The information criteria most relevant to competence are:

- Primary: effectiveness, efficiency and availability
- Secondary: confidentiality, integrity, compliance and reliability

1.4 Purpose of the Guideline

1.4.1 IS auditors are expected to be highly competent. To meet this objective, IS auditors need to acquire the necessary skills and required knowledge to carry out assignments. The additional challenge is to maintain competence by continually upgrading knowledge and skills.

1.4.2 By agreeing to provide professional services, IS auditors imply the availability of the desired level of competence required to perform professional services and that the knowledge and skill of the IS auditor will be applied with due care and diligence.

1.4.3 In view of the expectations of high competence, IS auditors should refrain from performing any services that they are not competent to carry out unless advice and assistance is obtained to provide reasonable assurance that the services are performed satisfactorily.

1.4.4 The IS auditor should perform professional services with due care, competence and diligence and has a continuing duty to maintain professional knowledge and skill at a required level to provide reasonable assurance that the requirements of professional auditing standards are met and the audited organisation receives the advantage of competent professional service based on up-to-date developments in practice, legislation and techniques.

1.4.5 ISACA's stated vision is to be the recognised global leader in IT governance, control and assurance. In the preface to the vision, it is clearly amplified that future success in the professions served by ISACA will require skills and competencies complementary to those measured by the CISA designation. ISACA is in the forefront of identifying these skills and competencies and devising ways to quantify and assess them. It is in this context that there is a need for a guideline to provide guidance to IS auditors to acquire necessary skills and knowledge and maintain competence while carrying out audit assignments.

1.4.6 This guideline provides guidance in applying IS auditing standard S4 (1006) Professional Competence. The IS auditor should consider this guideline in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

2. Responsibility

2.1 Skills and Knowledge

2.1.1 Primarily, the IS auditor should be responsible for acquiring the required professional and technical skills and knowledge to carry out any assignment the IS auditor agrees to perform.

2.1.2 Audit management has the secondary responsibility to entrust the audit assignment after ensuring that the IS auditor possesses the required professional and technical skills and knowledge to perform the tasks.

2.1.3 Audit management is responsible for ensuring that the team members performing the audit have the requisite skills and knowledge.

2.1.4 Skills and knowledge vary with the IS auditor's position and the role with respect to the audit. Requirement for management skills and knowledge should be commensurate with the level of responsibility

2.1.5 Skills and knowledge include proficiency in the identification and management of risks and controls, as well as audit tools and techniques. The IS auditor should possess analytical and technical knowledge together with interviewing, interpersonal and presentation skills.

2.2. Competence

2.2.1 Competence implies possessing skills and knowledge, and expertise through an adequate level of education and experience.

2.2.2 The IS auditor should provide reasonable assurance that he/she possesses the skills and knowledge necessary to attain the required level of competence.

2.2.3 The IS auditor should design the desired and/or expected level of competence based on appropriate benchmarks and such benchmarks are periodically reviewed and updated.

2.2.4 IS auditor and/or audit management should provide reasonable assurance of the availability of competent resources required to carry out any audit assignment prior to accepting the assignment/engagement, and the availability of such competent resources should be confirmed/ensured prior to commencement of an audit.

2.2.5 Audit management is responsible for ensuring the team members are competent to perform the audit assignment. Identification of core competencies of team members will assist in efficient utilisation of available resources.

2.2.6 It is considered appropriate for the IS auditors to share their experiences, adopted best practices, lessons learned and knowledge gained amongst team members to improve the competence of the resources. The competence of team members is also improved through team building sessions, workshops, conferences, seminars, lectures and other modes of interaction.

2.3 Continual Maintenance

2.3.1 The IS auditor should continually monitor their skills and knowledge to maintain the acceptable level of competence.

2.3.2 Maintenance through continuing professional education (CPE) may include, and is not limited to, training, educational courses, certification programmes, university courses, conferences, seminars, workshops, teleconferences, web casts and study circle meetings.

2.3.3 Acquiring skills and knowledge and maintaining competence levels should be monitored on a continual basis, and such skills, knowledge and competence should be evaluated periodically.

2.4 Evaluation

2.4.1 Evaluation should be carried out in a manner that is fair, transparent, easily understood, unambiguous, without bias and considered a generally acceptable practice given the respective employment environment.

2.4.2 Evaluation criteria and procedures should be clearly defined, but may vary depending upon circumstances such as geographic location, political climate, nature of assignment, culture and other similar circumstances.

2.4.3 In the case of an audit firm or a team of auditors, evaluation should be carried out internally amongst teams or individuals on a cross-functional basis.

2.4.4 In the case of a single (sole) independent IS auditor, evaluation should be carried out by a peer relationship to the extent possible. If a peer review is not possible, self-evaluation should be conducted and documented.

2.4.5 An appropriate level of management is required to evaluate the performance of the internal IS auditor and also, wherever appropriate and necessary, the performance of external IS auditor(s).

2.4.6 Gaps noted during evaluation should be addressed appropriately.

2.5 Gap Analysis and Training

2.5.1 Gaps noted based upon variances in the actual level of competence to the expected level of competence should be recorded and analysed. Where deficiency exists in any resource, such resources should not be utilised to conduct the audit assignment unless adequate measures to rectify the deficiency are undertaken. However, if the deficiency is noticed after commencement of the audit assignment, the IS auditor/audit management should consider withdrawing the deficient resource(s) and replacing it with a competent resource. However due to compulsions, if it is proposed to continue to use the resource for the continuance of the audit assignment, the existence of the gap should be communicated to the auditee. The concurrence of the auditee should be obtained for the continued use of the deficient resource, provided that the IS auditor is able to reasonably assure the quality of the audit.

2.5.2 It is important that the root cause analysis is performed to ascertain the reason for the gap and that appropriate corrective action measures, such as training, are conducted as soon as possible.

2.5.3 Training activities required for an audit engagement should be completed within a reasonable time and before commencement of the audit activity.

2.5.4 Effectiveness of training should be measured on completion of training after a reasonable time period.

2.6 Availability of Competent Resources

2.6.1 The IS auditor/audit management should understand and analyse the requirement of skills and knowledge of the proposed audit assignment, before responding to a request for proposal.

2.6.2 The IS auditor/audit management should provide reasonable assurance that requisite resources with the necessary skills, knowledge and required level of competency are available before commencing the audit assignments.

2.6.3 IS auditors should not portray themselves as having expertise, competence or experience they do not possess.

2.7 Outsourcing

2.7.1 Where any part of the audit assignment is outsourced or expert assistance obtained, it must be reasonable assurance must be provided that the external expert or the outsourced agency possesses the requisite competence. This guideline also applies for selection of an external expert.

2.7.2 Where expert assistance is obtained on a continual basis, competencies of such external experts should be measured and monitored/reviewed periodically.

3. Continuing Professional Education

3.1 Requirements of Professional Bodies

3.1.1 Continuing professional education (CPE) is the methodology adopted to maintain competence and update skills and knowledge.

3.1.2 IS auditors should adhere to the requirements of the CPE policies established by the respective professional bodies with which they are associated.

3.2 Eligible Programmes

3.2.1 CPE programmes should aid in the enhancement of skill and knowledge and must relate to professional and technical requirements of IS assurance, security and governance

3.2.2 Professional bodies ordinarily prescribe programmes eligible for CPE recognition. IS auditors should adhere to such norms prescribed by their respective professional bodies.

3.3 Attainment of CPE Credits

3.3.1 Professional bodies ordinarily prescribe the methodology of attainment of CPE credits and the minimum credits that should be obtained periodically by their constituents. IS auditors must adhere to such norms prescribed by their respective professional bodies.

3.3.2 Where the IS auditor is associated with more than one professional body for the purpose of attainment of minimum credits, the IS auditor may use his/her judgement to avail CPE credits in a common manner from the eligible programmes, provided the same is consistent with the rules/guidelines framed by the respective professional bodies.

3.4 ISACA's CPE Policy

3.4.1 ISACA has a comprehensive policy on continuing professional education, applicable to its members and holders of the CISA designation. IS auditors with the CISA designation must comply with ISACA's CPE policy. Details of the policy are available on the ISACA web site, *www.isaca.org/CISAcpePolicy*. The policy explains the criteria for:

- Certification requirements
- Verification of attendance form
- Code of Professional Ethics
- Audits of continuing professional education hours
- Revocation, reconsideration and appeal
- Retired and nonpracticing CISA status
- Qualifying educational activities
- Calculating continuing professional education hours

4. Records

4.1 Skill Matrix and Training Records

4.1.1 A skill matrix indicating the skill, knowledge and competence required for various job levels should be formulated. This matrix is cross-referenced to the available resources and their skill and knowledge. This matrix will aid in the identification of gaps and training needs.

4.1.2 Records of training provided, together with feedback on training and effectiveness of training, should be maintained, analysed and referenced for future use.

4.2 CPE Records

4.2.1 As prescribed by respective professional bodies, including ISACA, IS auditors are required to maintain appropriate records of CPE programmes, retain them for specific periods and, if required, make them available for audits.

5. Effective Date

5.1 This guideline is effective for all information systems audits beginning 1 June 2005. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

2007 Assertions (in development)

2008 Criteria (in development)

Performance Guidelines

The performance guidelines are:
2201 Engagement Planning (G15)
2202 Risk Assessment in Audit Planning (G13)
2203 Performance and Supervision (G8)
2204 Audit Materiality (G6)
2205 Using the Work of Other Experts (G1)
2206 Audit Evidence (G2)
2207 Irregularity and Illegal Acts (G9)
2208 Audit Sampling (G10)

The guidelines are included here in their entirety. For links to the individual standards, visit *www.isaca.org/standard*.

2201 Engagement Planning (G15)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S5 (1201) Planning states that IT audit and assurance professionals should plan the information systems (IS) audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards. They should develop and document:
- A risk-based audit approach
- An audit plan that details the nature and objectives, timing and extent, objectives, and resources required
- An audit programme and/or plan detailing the nature, timing and extent of the audit procedures required to complete the audit

1.1.2 Standard S11 (1202) Use of Risk Assessment in Audit Planning states that IT audit and assurance professionals should:
- Use an appropriate risk assessment technique or approach in developing the overall IT audit plan and in determining priorities for the effective allocation of IT audit resources
- When planning individual reviews, identify and assess risks relevant to the area under review and its relationship to other auditable areas

1.1.3 Standard S12 (1204) Audit Materiality states that the IT audit and assurance professionals should consider:
- Audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures
- While planning for an audit, potential weaknesses or absences of controls and whether such weaknesses or absences of controls could result in significant deficiency or a material weakness in the information system
- The cumulative effect of minor control deficiencies or weaknesses and absences of controls to translate into significant deficiency or material weakness in the information system

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the planning requirements of IT audit and assurance professionals, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The processes and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.3 Primary IT processes are:
- ME1 *Monitor and evaluate IT performance*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure compliance with external requirements*

1.2.4 Secondary IT process is:
- ME4 *Provide IT governance*

1.2.5 The information criteria most relevant are:
- Primary: Effectiveness, efficiency, availability and compliance
- Secondary: Confidentiality, integrity and reliability

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to define the components of the planning process as stated in standard S5 (1201) of *ITAF: A Professional Practices Framework for IT Assurance*.

1.3.2 This guideline also provides for planning in the audit process to meet the objectives set by COBIT.

2. Preliminary Engagement Activities

2.1 Purpose

2.1.1 The purpose of performing these preliminary engagement activities is to help ensure that IT audit and assurance professionals have considered any events or circumstances that may adversely affect their ability to plan and perform the audit engagement and reduce audit risk to an acceptably low level. Performing these preliminary engagement activities helps to ensure the audit engagement plans include that:
- IT audit and assurance professionals maintain the necessary independence and ability to perform the engagement
- There are no issues with management integrity that may affect IT audit and assurance professionals' willingness to continue the engagement
- There is no misunderstanding with the clients as to the terms of the engagement

2.2 Activities

2.2.1 IT audit and assurance professionals should perform procedures regarding the continuance of the client relationship and the specific audit engagement. For continuing audit engagements, such initial procedures often occur shortly after (or in connection with) the completion of the previous audit.

2.2.2 IT audit and assurance professionals should evaluate compliance with ethical requirements, including independence. IT audit and assurance professionals' initial procedures on both clients' continuance and evaluation of ethical requirements (including independence) are performed prior to performing other significant activities for the current audit engagement.

2.2.3 IT audit and assurance professionals should establish an understanding of the terms of the engagement.

3. Planning

3.1 Audit Strategy

3.1.1 IT audit and assurance professionals should plan the engagement, so that it will be performed in an effective manner, and establish the overall audit strategy for the audit. Adequate planning helps to ensure that appropriate attention is devoted to important areas of the audit, potential problems are identified and resolved on a timely basis, and the audit engagement is properly organised and managed to be performed in an effective and efficient manner.

3.1.2 A clear project definition is a critical success factor to ensure project effectiveness and efficiency. An audit project should include in the terms of reference such items as:

- Areas to be audited
- Type of work planned
- High-level objectives and scope of the work
- Topics, e.g., budget, resource allocation, schedule dates, type of report, intended audience
- Other general aspects of the work, when applicable

3.1.3 For an internal audit function, a comprehensive risk-based audit plan should be developed/updated, at least annually, for ongoing activities. This high-level plan should act as a framework for audit activities and serve to address responsibilities set by the audit charter.

3.1.4 A plan should normally be prepared for each audit assignment. The plan should document the objectives of the audit.

3.1.5 Each audit project should be referenced either to the general audit plan or state the specific mandate, objectives and other relevant aspects of the work to be performed.

3.1.6 IT audit and assurance professionals should develop an audit plan that takes into consideration the objectives of the auditee relevant to the audit area and the related technology infrastructure. Where appropriate, they should also consider the area under review and its relationship to the enterprise (strategically, financially and/or operationally) and obtain information on the strategic plan, including the IT strategic plan and any other relevant documentation related to the auditee.

3.1.7 IT audit and assurance professionals should have an understanding of the auditee's information architecture and the auditee's technological direction to be able to design a plan appropriate for the present and, where appropriate, future technology of the auditee.

3.2 Knowledge of the Enterprise

3.2.1 Understanding the auditee´s business and the risks it faces is a critical step to developing an effective audit plan focused on the areas most sensitive to fraudulent or inaccurate practices.

3.2.2 Before beginning an audit project, the work of IT audit and assurance professionals should be planned in a manner appropriate for meeting the audit objectives. As a part of the planning process, they should obtain an understanding of the enterprise and its processes. In addition to giving IT audit and assurance professionals an understanding of the enterprise's operations and its IT requirements, this will assist them in determining the significance of the IT resources being reviewed as they relate to the objectives of the enterprise. IT audit and assurance professionals should also establish the scope of the audit work and perform a preliminary assessment of internal control over the function being reviewed.

3.2.3 The extent of the knowledge of the enterprise and its processes required by IT audit and assurance professionals will be determined by the nature of the enterprise and the level of detail at which the audit work is being performed. IT audit and assurance professionals may require specialized knowledge when dealing with unusual or complex operations. A more extensive knowledge of the enterprise and its processes will ordinarily be required when the audit objective involves a wide range of IT functions, rather than when the objectives are for limited functions. For example, a review with the objective of evaluating control over an enterprise's payroll system would ordinarily require a more thorough understanding of the enterprise than a review with the objective of testing controls over a specific programme library system.

3.2.4 IT audit and assurance professionals should gain an understanding of the types of personnel, events, transactions and practices that can have a significant effect on the specific enterprise, function, process or data that is the subject of the auditing project. Knowledge of the enterprise should include the business, financial and inherent risks facing the enterprise as well as conditions in the enterprise's marketplace and the extent to which the enterprise relies on outsourcing to meet its objectives. IT audit and assurance professionals should use this information in identifying potential problems, formulating the objectives and scope of the work, performing the work, and considering actions of management for which they should be alert.

3.3 Materiality

3.3.1 In the planning process, IT audit and assurance professionals should ordinarily establish levels of planning materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently. For example, in the review of an existing system, the IT audit and assurance professional will evaluate materiality of the various components of the system in planning the audit programme for the work to be performed. Both qualitative and quantitative aspects should be considered in determining materiality.

3.4 Risk Assessment

3.4.1 The IT audit and assurance professionals should develop an audit plan for the audit to reduce audit risk to an acceptably level.

3.4.2 A risk assessment should be performed to provide reasonable assurance that all material items will be adequately covered during the audit work. This assessment should identify areas with relatively high probability of material problems.

3.4.3 A risk assessment and prioritisation of identified risks for the area under review and the Enterprise's IT environment should be carried out to the extent necessary.

3.5 Internal Control Evaluation

3.5.1 Audit and assurance projects should include consideration of internal controls either directly as a part of the project objectives or as a basis for reliance upon information being gathered as a part of the project. Where the objective is evaluation of internal controls, IT audit and assurance professionals should consider the extent to which it will be necessary to review such controls. When the objective is to assess the effectiveness of controls over a period of time, the audit plan should include procedures appropriate for meeting the audit objectives, and these procedures should include compliance testing of controls. When the objective is not to assess the effectiveness of controls over a period of time, but rather to identify control procedures at a point in time, compliance testing of controls may be excluded.

3.5.2 When IT audit and assurance professionals evaluate internal controls for the purpose of placing reliance on control procedures in support of information being gathered as part of the audit, they should ordinarily make a preliminary evaluation of the controls and develop the audit plan on the basis of this evaluation. During a review, IT audit and assurance professionals should consider the appropriateness of this evaluation in determining the extent to which controls can be relied upon during testing. For example, in using a computer program to test data files, the IT audit and assurance professional should evaluate controls over program libraries containing programs being used for audit purposes to determine the extent to which the programs are protected from unauthorised modification.

4. Changes During the Course of the Audit

4.1 Strategy and Planning

4.1.1 The overall audit strategy and the audit plan should be updated and changed as necessary during the course of the audit.

4.1.2 Planning an audit is a continual and iterative process. As a result of unexpected events, changes in conditions or the audit evidence obtained from the results of audit procedures, the IT audit and assurance professionals may need to modify the overall audit strategy and the resulting planned nature, timing and extent of further audit procedures.

4.1.3 The audit planning should consider the possibility of unexpected events that implicate high risks for the enterprise. Therefore, the audit plan must be able to prioritise such events within the audit and assurance processes in a risk-adequate manner.

5. Supervision

5.1 Engagement Team Members

5.1.1 IT audit and assurance professionals should plan the nature, timing and extent of direction and supervision of engagement team members and review their work. That planning depends on many factors, including the size and complexity of the enterprise, the area of audit, the risks of material misstatement, the capabilities and competence of personnel performing the audit work, and the extent of direction and supervision of engagement team members based on the assessed risk of material misstatement.

6. Documentation

6.1 Planning Documentation

6.1.1 The IT audit and assurance professional's work papers should include the audit plan and programme.

6.1.2 The audit plan may be documented on paper or in another appropriate and retrievable form.

6.2 Plan Endorsement

6.2.1 To the extent appropriate, the audit plan, audit programme and any subsequent changes should be approved by audit management.

6.3 Audit Programme

6.3.1 A preliminary programme for review should ordinarily be established by the IT audit and assurance professional before the start of work. This audit programme should be documented in a manner that will permit the IT audit and assurance professional to record completion of the audit work and identify work that remains to be done. As the work progresses, the IT audit and assurance professional should evaluate the adequacy of the programme based on information gathered during the audit. When IT audit and assurance professionals determine that the planned procedures are not sufficient, they should modify the programme accordingly.

6.3.2 Depending on the audit resources required, the IT audit and assurance professional should include management of the personnel resources required in the audit plan.

6.3.3 The audit plan should be prepared so that it is in compliance with any appropriate external requirements in addition to the standards as defined in ITAF.

6.3.4 In addition to a listing of the work to be done, the IT audit and assurance professional should, to the extent practicable, prepare a list of personnel and other resources required to complete the work, a schedule for the work, and a budget.

6.3.5 The audit programme and/or plan should be adjusted during the course of the audit to address issues that arise (new risks, incorrect assumptions, or findings from the procedures already performed) during the audit.

7. Effective Date

7.1 This guideline is effective for all IT audits beginning after 1 May 2010.

2202 Risk Assessment in Audit Planning (G13)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S5 (1201) Planning states: 'The IS auditor should plan the IS audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.2 Standard S6 (1203) Performance of Audit Work states: 'During the course of the audit, the IS auditor should obtain sufficient and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.1.3 Paragraph 2.4.1 of IS Auditing Guideline G15 (2201) Planning states: 'An assessment of risk should be made to provide reasonable assurance that material items will be covered adequately during the audit work. This assessment should identify areas with relatively high risk of existence of material problems'.

1.2 Linkage to Procedures

1.2.1 This guideline may be used in conjunction with IS Auditing Procedure P1 IS Risk Assessment Measurement (withdrawn).

1.3 Linkage to COBIT

1.3.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the audit documentation requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary.

1.3.2 PO9 *Assess and manage IT risks* satisfies the business requirement for IT of analysing and communicating IT risks and their potential impact on business processes and goals by focusing on development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk.

1.3.2 ME2 *Monitor and Evaluate Internal Control* satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws, regulations and contracts by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.3.5 Secondary references:

- ME3 *Ensure regulatory compliance*
- ME4 *Provide IT governance*

1.3.6 The information criteria most relevant are:

- Primary: Confidentiality, integrity, availability
- Secondary: Effectiveness, efficiency, compliance and reliability

1.4 Need for Guideline

1.4.1 The level of audit work required to meet a specific audit objective is a subjective decision made by the IS auditor. The risk of reaching an incorrect conclusion based on the audit findings (audit risk) is one aspect of this decision. The other is the risk of errors occurring in the area being audited (error risk). Recommended practices for risk assessment in carrying out financial audits are well documented in auditing standards for financial auditors, but guidance is required on how to apply such techniques to IS audits.

1.4.2 Members of management also bases their decisions on how much control is appropriate upon assessment of the level of risk exposure that they are prepared to accept. For example, the inability to process computer applications for a period of time is an exposure that could result from unexpected and undesirable events (e.g., data centre fire). Exposures can be reduced by the implementation of appropriately designed controls. These controls are ordinarily based upon probabilistic estimation of the occurrence of adverse events and are intended to decrease such probability. For example, a fire alarm does not prevent fires, but it is intended to reduce the extent of fire damage.

1.4.3 This guideline provides guidance in applying IS Auditing Standards. The IS auditor should consider it in determining how to achieve implementation of standards S5 (1201) and S6 (1203) , use professional judgement in its application, and be prepared to justify any departure.

2. Planning

2.1 Selection of a Risk Assessment Methodology

2.1.1 There are many risk assessment methodologies available from which the IS auditor may choose. These range from simple classifications of high, medium and low, based on the IS auditor's judgement, to complex and apparently scientific calculations to provide a numeric risk rating. IS auditors should consider the level of complexity and detail appropriate for the organisation being audited.

2.1.2 IS auditors should include, at a minimum, an analysis, within the methodology, of the risks to the enterprise resulting from the loss of and controls supporting system availability, data integrity and business information confidentiality.

2.1.3 All risk assessment methodologies rely on subjective judgements at some point in the process (e.g., for assigning weightings to the various parameters). The IS auditor should identify the subjective decisions required to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.

2.1.4 In deciding which is the most appropriate risk assessment methodology, IS auditors should consider such things as:

- The type of information required to be collected (some systems use financial effects as the only measure—this is not always appropriate for IS audits)
- The cost of software or other licences required to use the methodology
- The extent to which the information required is already available
- The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
- The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits
- The willingness of management to accept the methodology as the means of determining the type and level of audit work carried out

2.1.5 No single risk assessment methodology can be expected to be appropriate in all situations. Conditions affecting audits may change over time. Periodically, the IS auditor should re-evaluate the appropriateness of the chosen risk assessment methodologies.

2.2 Use of Risk Assessment

2.2.1 IS auditors should use the selected risk assessment techniques in developing the overall audit plan and in planning specific audits. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as:

- The nature, extent and timing of audit procedures
- The areas or business functions to be audited
- The amount of time and resources to be allocated to an audit

2.2.2 The IS auditor should consider each of the following types of risk to determine their overall level:

- Inherent risk
- Control risk
- Detection risk

2.3 Inherent Risk

2.3.1 Inherent risk is the susceptibility of an audit area to error in a way that could be material, individually or in combination with other errors, assuming that there were no related internal controls. For example, the inherent risk associated with operating system security is ordinarily high, since changes to, or even disclosure of, data or programs through operating system security weaknesses could result in false management information or competitive disadvantage. By contrast, the inherent risk associated with security for a stand-alone PC, when a proper analysis demonstrates it is not used for business-critical purposes, is ordinarily low.

2.3.2 Inherent risk for most IS audit areas is ordinarily high since the potential effects of errors ordinarily spans several business systems and many users.

2.3.3 In assessing the inherent risk, the IS auditor should consider both pervasive and detailed IS controls. This does not apply to circumstances where the IS auditor's assignment is related to pervasive IS controls only.

2.3.4 At the pervasive IS control level, the IS auditor should consider, to the level appropriate for the auditarea in question:

- The integrity of IS management and IS management experience and knowledge
- Changes in IS management
- Pressures on IS management that may predispose them to conceal or misstate information (e.g., large business-critical project overruns, hacker activity)
- The nature of the organisation's business and systems (e.g., the plans for e-commerce, the complexity of the systems, the lack of integrated systems)
- Factors affecting the organisation's industry as a whole (e.g., changes in technology, IS staff availability)
- The level of third-party influence on the control of the systems being audited (e.g., because of supply chain integration, outsourced IS processes, joint business ventures, and direct access by customers)
- Findings from and date of previous audits

2.3.5 At the detailed IS control level, the IS auditor should consider, to the level appropriate for the audit area in question:

- The findings from and date of previous audits in this area
- The complexity of the systems involved
- The level of manual intervention required
- The susceptibility to loss or misappropriation of the assets controlled by the system (e.g., inventory, payroll)
- The likelihood of activity peaks at certain times in the audit period
- Activities outside the day-to-day routine of IS processing (e.g., the use of operating system utilities to amend data)
- The integrity, experience and skills of management and staff involved in applying the IS controls

2.4 Control Risk

2.4.1 Control risk is the risk that an error that could occur in an audit area and could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often missed easily, owing to the volume of logged information. The control risk associated with computerised data validation procedures is ordinarily low because the processes are consistently applied.

2.4.2 The IS auditor should assess the control risk as high unless relevant internal controls are:

- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

2.5 Detection Risk

2.5.1 Detection risk is the risk that the IS auditor's substantive procedures will not detect an error that could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with identifying a lack of disaster recovery plans is ordinarily low, since existence is verified easily.

2.5.2 In determining the level of substantive testing required, IS auditors should consider both:

- The assessment of inherent risk
- The conclusion reached on control risk following compliance testing

2.5.3 The higher the assessment of inherent and control risk the more audit evidence IS auditors should normally obtain from the performance of substantive audit procedures.

3. Performance of Audit Work

3.1 Documentation

3.1.1 IS auditors should consider documenting the risk assessment technique or methodology used for a specific audit. The documentation should ordinarily include:

- A description of the risk assessment methodology used
- The identification of significant exposures and the corresponding risks
- The risks and exposures the audit is intended to address
- The audit evidence used to support the IS auditor's assessment of risk

4. Effective Date

4.1 This guideline is effective for all IS audits beginning on or after 1 September 2000. The guideline has been reviewed and updated effective 1 August 2008.

2203 Performance and Supervision (G8)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S5 (1201) Planning, states 'The IS auditor document an audit plan that lists the audit detailing the nature and objectives, timing and extent, objectives and resources required'.

1.1.2 Standard S6 (1203) Performance of Audit Work, states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence. The audit process should be documented, describing the audit work performed and the audit evidence that supports the IS auditor's findings and conclusions'.

1.1.3 Standard S7 (1401) Reporting, states 'The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The audit report should state the scope, objectives, period of coverage, and the nature, timing and extent of the audit work performed. The report should state the findings, conclusions, recommendations, and any reservations, qualifications or limitations that the IS auditor has with respect to the audit. When issued, the IS auditor's report should be signed, dated and distributed according to the terms of the audit charter or engagement letter'.

1.1.4 Standard S12 (1204) Audit Materiality, states 'The report of the IS auditor should disclose ineffective controls or absence of controls and the significance of the control deficiencies and possibility of these weaknesses resulting in a significant deficiency or material weakness'.

1.1.5 Standard S13 (1205) Using the Work of Other Experts, states 'The IS auditor should determine whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives. Such conclusion should be clearly documented'.

1.2 Linkage to COBIT

1.2.1 PO1 *Define a strategic IT plan*, satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks by focusing on incorporating IT and business management in the translation of business requirements into service offerings and the development of strategies to deliver these services in a transparent and effective manner.

1.2.2 PO8 *Manage quality*, satisfies the business requirement for IT of continuous and measurable improvement of the quality of IT services delivered by focusing on the definition of a quality management system (QMS), ongoing performance monitoring against predefined objectives and implementation of a programme for continuous improvement of IT services.

1.2.3 AI6 *Manage changes*, satisfies the business requirement for IT of responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework by focusing on controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications, and halting implementation of unauthorised changes.

1.2.4 DS1 *Define and manage service*, satisfies the business requirement for IT of ensuring the alignment of key IT services with business strategy by focusing on identifying service requirements, agreeing on service levels and monitoring the achievement of service levels.

1.2.5 ME2 *Monitor and evaluate internal control*, satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws and regulations by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.2.6 ME3 *Ensure regulatory compliance*, satisfies the business requirement for IT of compliance with laws and regulations by focusing on identifying all applicable laws and regulations and the corresponding level of IT compliance and optimising IT processes to reduce the risk of noncompliance.

1.2.7 The information criteria most relevant are:

- Primary: Reliability, availability, efficiency and integrity
- Secondary: Effectiveness and confidentiality

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to describe the documentation that the IS auditor should prepare and retain to support the audit.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

2. Planning And Performance

2.1 Documentation Contents

2.1.1 IS audit documentation is the record of the audit work performed and the audit evidence supporting the IS auditor's findings, conclusions and recommendations. Audit documentation should be complete, clear, structured, indexed, and easy to use and understand by the reviewer. Potential uses of documentation include, but are not limited to:

- Demonstration of the extent to which the IS auditor has complied with the IS Auditing Standards
- Demonstration of audit performance to meet requirements as per the audit charter
- Assistance with planning, performance and review of audits
- Facilitation of third-party reviews
- Evaluation of the IS auditing function's QA programme
- Support in circumstances such as insurance claims, fraud cases, disputes and lawsuits
- Assistance with professional development of staff

2.1.2 Documentation should include, at a minimum, a record of:

- Review of previous audit documentation
- The planning and preparation of the audit scope and objectives. IS auditors must have an understanding of the industry, business domain, business process, product, vendor support and overall environment under review.
- Minutes of management review meetings, audit committee meetings and other audit-related meetings
- The audit programme and audit procedures that will satisfy the audit objectives
- The audit steps performed and audit evidence gathered to evaluate the strengths and weakness of controls
- The audit findings, conclusions and recommendations
- Any report issued as a result of the audit work
- Supervisory review

2.1.3 The extent of the IS auditor's documentation depends on the needs for a particular audit and should include such things as:

- The IS auditor's understanding of the areas to be audited and its environment.
- The IS auditor's understanding of the information processing systems and the internal control environment including the:
  - Control environment
  - Control procedures
  - Detection risk assessment
  - Control risk assessment
  - Equate total risk
- The author and source of the audit documentation and the date of its completion
- Methods used to assess adequacy of control, existence of control weakness or lack of controls, and identify compensating controls
- Audit evidence, the source of the audit documentation and the date of completion, including:
  - Compliance tests, which are based on test policies, procedures and segregation duties
  - Substantive tests, which are based on analytic procedures, detailed test accounts balances and other substantive audit procedures
- Acknowledgement from appropriate person of receipt of audit report and findings
- Auditee's response to recommendations
- Version control, especially where documentation is in electronic media

2.1.4 Documentation should include appropriate information required by law, government regulations or applicable professional standards.

2.1.5 Documentation should be submitted to the audit committee for its review and approval.

3. Documentation

3.1 Custody, Retention and Retrieval

3.1.1 Policies and procedures should be in effect to verify and ensure appropriate custody and retention of the documentation that supports audit findings and conclusions for a period sufficient to satisfy legal, professional and organisational requirements.

3.1.2 Documentation should be organised, stored and secured in a manner appropriate for the media on which it is retained and should continue to be readily retrievable for a time sufficient to satisfy the policies and procedures defined above.

4. Effective Date

4.1. This revised guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 March 2008.

2204 Audit Materiality (G6)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S5 (1201) Planning states, 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.2 Standard S10 IT Governance (withdrawn), states 'The IS auditor should review and assess compliance with legal, environmental, information quality, fiduciary and security requirements'.

1.1.3 Standard S12 (1204) Audit Materiality, states 'The IS auditor should consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures. While planning for audit, the IS auditor should consider potential weakness or absence of controls and whether such weakness or absence of controls could result into significant deficiency or a material weakness in the information system. The IS auditor should consider the cumulative effect of minor control deficiencies or weaknesses and the absence of controls to translate into significant deficiency or material weakness in the information system'.

1.1.4 Standard S9 (1207) Irregularities and Illegal Acts, states 'If the IS auditor has identified a material irregularity or illegal act involving management or employees who have significant roles in internal control, or obtains information that a material irregularity or illegal act may exist, the IS auditor should communicate these matters to the appropriate level of management in a timely manner'.

1.2 Linkage to COBIT

1.2.1. PO5 *Manage the IT investment* 'satisfies the business requirement for IT of continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardised services that satisfy end-user expectations by focusing on effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions'.

1.2.2 AI1 *Identify automated solutions* 'satisfies the business requirement for IT of translating business functional and control requirements into an effective and efficient design of automated solutions by focusing on identifying technically feasible and cost-effective solutions'.

1.2.3 DS10 *Manage problems* 'satisfies the business requirement for IT of ensuring end users' satisfaction with service offerings and service levels; reducing solution and service delivery defects and rework by focusing on recording, tracking and resolving operational problems; investigating the root cause of all significant problems; and defining solutions for identified operations problems'.

1.2.4 DS13 *Manage operations* 'satisfies the business requirement for IT of maintaining data integrity and ensuring IT infrastructure can resist and recover from errors and failures by focusing on meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring and maintaining infrastructure'.

1.2.5 ME4 *Provide IT governance* 'satisfies the business requirement for IT of integrating IT governance with corporate governance objectives; complying with laws and regulations by focusing on preparing board reports on IT strategy, performance and risks; and responding to governance requirements in line with board directions'.

1.2.6 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the materiality concept of auditing information systems by the IS auditor, the processes in COBIT most likely to be relevant, selected and adapted are classified as primary and secondary as follows. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.7 Secondary references:

- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI4 *Enable operation and use*
- AI5 *Procure IT resources*
- AI6 *Manage changes*
- DS3 *Manage performance and capacity*
- DS5 *Ensure systems security*
- DS9 *Manage the configuration*
- ME1 *Monitor and evaluate IT performance*
- ME2 *Monitor and evaluate internal control*

1.2.8 The information criteria most relevant to audit materiality are:

- Primary: Confidentiality, integrity, compliance, reliability
- Secondary: Effectiveness, efficiency, availability

2. Need for Guideline

2.1 IS vs. Financial Audits

2.1.1 Unlike financial auditors, IS auditors require a different yardstick to measure materiality. Financial auditors ordinarily measure materiality in monetary terms, since what they audit is also measured and reported in monetary terms. IS auditors ordinarily perform audits of non-financial items, e.g., physical access controls, logical access controls, program change controls, and systems for personnel management, manufacturing control, design, quality control, password generation, credit card production and patient care. Therefore, IS auditors may need guidance on how materiality should be assessed to plan their audits effectively, how to focus their effort on high-risk areas and how to assess the severity of any errors or weaknesses found.

2.1.2 This guideline provides guidance in applying IS auditing standards on audit materiality. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

3. Planning

3.1 Assessing Materiality

3.1.1 The assessment of what is material is a matter of professional judgement and includes consideration of the effect and/or the potential effect on the organisation's ability to meet its business objectives in the event of errors, omissions, irregularities and illegal acts that may arise as a result of control weaknesses in the area being audited.

3.1.2 While assessing materiality, the IS auditor should consider:
- The aggregate level of error acceptable to management, the IS auditor, appropriate regulatory agencies and other stakeholders
- The potential for the cumulative effect of small errors or weaknesses to become material

3.1.3 To meet the audit objectives, the IS auditor should identify the relevant control objectives and, based on risk tolerance rate, determine what should be examined. With respect to a specific control objective, a material control is a control or group of controls without which control procedures do not provide reasonable assurance that the control objective will be met.

3.1.4 Where the IS audit objective relates to systems or operations that process financial transactions, the financial auditor's measure of materiality should be considered while conducting the IS audit.

3.1.5 The IS auditor should determine establishment of roles and responsibilities as well as a classification of information assets in terms of confidentiality, availability and integrity; access control rules on privileges management; and classification of information based upon degree of criticality and risk of exposure. Assessment should include verification of:
- Information stored
- IS hardware
- IS architecture and software
- IS network infrastructure
- IS operations
- Development and test environment

3.1.6 The IS auditor should determine whether any IT general deficiency could potentially become material. The significance of such deficient IT general controls should be evaluated in relation to their effect on application controls, i.e., whether the associated application controls are also ineffective. If the application deficiency is caused by the IT general control, then they are material. For example, if an application-based tax calculation is materially wrong and was caused by poor change controls to tax tables, then the application-based control (calculation) and the general control (changes) are materially weak.

3.1.7 The IS auditor should evaluate an IT general control's deficiency in relation to its effect on application controls and when aggregated against other control deficiencies. For example, a management decision not to correct an IT general control deficiency and its associated reflection on the control environment could become material when aggregated with other control deficiencies affecting the control environment.

3.1.8 The IS auditor should also note that failure to remediate a deficiency could become material.

3.1.9 The IS auditor should consider obtaining sign-off from appropriate stakeholders acknowledging they have disclosed existing material weakness that they are aware of in the organisation.

3.1.10 The following are examples of measures that should be considered to assess materiality:
- Criticality of the business processes supported by the system or operation
- Criticality of the information databases supported by the system or operation
- Number and type of application developed
- Number of users who use the information systems
- Number of managers and directors who work with the information systems classified by privileges
- Criticality of the network communications supported by the system or operation
- Cost of the system or operation (hardware, software, staff, third-party services, overheads or a combination of these)
- Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage, etc.)

- Cost of loss of critical and vital information in terms of money and time to reproduce
- Effectiveness of countermeasures
- Number of accesses/transactions/inquiries processed per period
- Nature, timing and extent of reports prepared and files maintained
- Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)
- Service level agreement requirements and cost of potential penalties
- Penalties for failure to comply with legal, regulatory and contractual requirements
- Penalties for failure to comply with public health and safety requirements

3.1.11 Control failures may potentially lead to monetary loss, competitive position, loss of trust or loss of reputation, apart from damaging the corporate image. The IS auditor should evaluate risks against possible countermeasures.

4. Reporting

4.1 Identifying Reportable Issues

4.1.1 In determining the findings, conclusions and recommendations to be reported, the IS auditor should consider both the materiality of any errors found and the potential materiality of errors that could arise as a result of control weaknesses.

4.1.2 Where the audit is used by management to obtain a statement of assurance regarding IS controls, an unqualified opinion on the adequacy of controls should mean that the controls in place are in accordance with generally accepted control practices to meet the control objectives, devoid of any material control weakness.

4.1.3 A control weakness should be considered material and, therefore, reportable, if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. If the audit work identifies material control weaknesses, the IS auditor should consider issuing a qualified or adverse opinion on the audit objective.

4.1.4 Depending on the objectives of the audit, the IS auditor should consider reporting to management weaknesses that are not material, particularly when the costs of strengthening the controls are low.

5. Effective Date

5.1 This guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 May 2008.

2205 Audit Evidence (G2)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S6 (1203) Performance of Audit Work states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.1.2 Standard S9 (1207) Irregularities and Illegal Acts states 'The IS auditor should obtain sufficient and appropriate evidence to determine whether management or others within the organization have knowledge of actual, suspected or alleged irregularities and illegal acts'.

1.1.3 Standard S13 (1205) Using the Work of Other Experts states 'The IS auditor should provide appropriate audit opinion and include scope limitation where required evidence is not obtained through additional test procedures'.

1.1.4 Standard S14 (1206) Audit Evidence states 'The IS auditor should obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the audit results. The IS auditor should evaluate the sufficiency of audit evidence obtained during the audit'.

1.1.5 Procedure P7 Irregularities and Illegal Acts (withdrawn) states "Although the IS auditor has no explicit responsibility to detect or prevent irregularities, the IS auditor should assess the level of risk that irregularities could occur. The result of the risk assessment and other procedures performed during planning should be used to determine the nature, extent and timing of the procedures performed during the engagement'.

1.2 Linkage to COBIT

1.2.1 ME2.3 *Control exceptions states* 'Record information regarding all control exceptions and ensure that it leads to analysis of the underlying cause and to corrective action. Management should decide which exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Management is also responsible to inform affected parties'.

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to guide the IS auditor to obtain sufficient and appropriate audit evidence and draw reasonable conclusions on which to base the audit results.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

2. Planning

2.1 Types of Audit Evidence

2.1.1 For a description of appropriate, reliable and sufficient evidence, refer to the commentary section in standard S14 (1206).

2.1.2 When planning the IS audit work, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability. Amongst the things to be considered are the independence and qualifications of the provider of the audit evidence. For example, corroborative audit evidence from an independent third party can be more reliable than audit evidence from the organisation being audited. Physical audit evidence is generally more reliable than the representations of an individual.

2.1.3 The IS auditor should also consider whether testing of controls has been completed and attested to by an independent third party and whether any reliance can be placed on that testing.

2.1.4 The various types of audit evidence that the IS auditor should consider using include:

- Observed processes and existence of physical items
- Documentary audit evidence
- Representations
- Analysis

2.1.5 Observed processes and existence of physical items can include observations of activities, property and IS functions, such as:

- An inventory of media in an offsite storage location
- A computer room security system in operation

2.1.6 Documentary audit evidence, recorded on paper or other media, can include:

- Results of data extractions
- Records of transactions
- Program listings
- Invoices
- Activity and control logs
- System development documentation

2.1.7 Representations of those being audited can be audit evidence, such as:

- Written policies and procedures
- System flowcharts
- Written or oral statements

2.1.8 The results of analysing information through comparisons, simulations, calculations and reasoning can also be used as audit evidence. Examples include:
- Benchmarking IS performance against other organisations or past periods
- Comparison of error rates between applications, transactions and users

2.2 Availability of Audit Evidence

2.2.1 The IS auditor should consider the time during which information exists or is available in determining the nature, timing, extent of substantive testing and, if applicable, compliance testing. For example, audit evidence processed by electronic data interchange (EDI), document image processing (DIP) and dynamic systems such as spreadsheets may not be retrievable after a specified period of time if changes to the files are not controlled or the files are not backed up. Documentation availability could also be impacted by company document retention policies.

2.3 Selection of Audit Evidence

2.3.1 The IS auditor should plan to use the most appropriate, reliable and sufficient audit evidence attainable and consistent with the importance of the audit objective and the time and effort involved in obtaining the audit evidence.

2.3.2 Where audit evidence obtained in the form of oral representations is critical to the audit opinion or conclusion, the IS auditor should consider obtaining documentary confirmation of the representations, either on paper or other media. The auditor should also consider alternative evidence to corroborate these representations to ensure their reliability.

3. Performance of Audit Work

3.1 Nature of Audit Evidence

3.1.1 Audit evidence should be sufficient, reliable, relevant and useful to form an opinion or support the IS auditor's findings and conclusions. If, in the IS auditor's judgement, the audit evidence obtained does not meet these criteria, the IS auditor should obtain additional audit evidence. For example, a program listing may not be adequate audit evidence until other audit evidence has been gathered to verify that it represents the actual program used in the production process.

3.2 Gathering Audit Evidence

3.2.1 Procedures used to gather audit evidence vary depending on the information system being audited. The IS auditor should select the most appropriate, reliable and sufficient procedure for the audit objective. The following procedures should be considered:
- Inquiry
- Observation
- Inspection
- Confirmation
- Reperformance
- Monitoring

3.2.2 The above can be applied through the use of manual audit procedures, computer-assisted audit techniques, or a combination of both. For example:
- A system which uses manual control totals to balance data entry operations might provide audit evidence that the control procedure is in place by way of an appropriately reconciled and annotated report. The IS auditor should obtain audit evidence by reviewing and testing this report.
- Detailed transaction records may only be available in machine-readable format requiring the IS auditor to obtain audit evidence using computer-assisted audit techniques. The auditor should ensure that the version or type(s) of computer-assisted audit techniques (CAATs) to be used are updated and/or fully compatible with the format(s) structured for the detailed transaction records in question.

3.2.3 If there is a possibility that the gathered evidence will become part of a legal proceeding, the IS auditor should consult with the appropriate legal counsel to determine whether there are any special requirements that will impact the way evidence needs to be gathered, presented and disclosed.

3.3 Audit Documentation

3.3.1 Audit evidence gathered by the IS auditor should be appropriately documented and organised to support the IS auditor's findings and conclusions.

3.3.2 For a discussion on protection and retention of evidence, refer to the commentary section in standard S14 (1206).

4. Reporting

4.1 Restriction of Scope

4.1.1 In those situations where the IS auditor believes sufficient audit evidence cannot be obtained, the IS auditor should disclose this fact in a manner consistent with the communication of the audit results.

5. Effective Date

5.1 This guideline is effective for all information systems audits beginning on or after 1 December 1998. The guideline has been reviewed and updated effective 1 May 2008

2206 Using the Work of Other Experts (G1)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S13 (1205) Using the Work of Other Experts states 'The IS auditor should, where appropriate, consider using the work of other experts for the audit'.

1.1.2 Standard S6 (1203) Performance of Audit Work states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to COBIT

1.2.1 ME2.5 states that the IS auditor should 'Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews. Such reviews may be conducted by the corporate compliance function or, at management's request, by internal audit or commissioned to external auditors and consultants or certification bodies. Qualifications of individuals performing the audit, e.g., CISA® certification, must be ensured.'

1.3 Need for Guideline

1.3.1 The interdependency of customers' and suppliers' processing and the outsourcing of non-core activities mean that an IS auditor (internal or external) will often find that parts of the environment being audited are controlled and audited by other independent functions or organisations. This guideline sets out how the IS auditor should comply with the above standard in these circumstances. Compliance with this guideline is not mandatory, but the IS auditor should be prepared to justify deviation from it.

1.3.2 IS auditors should consider using the work of other experts in the audit when there are constraints that could impair the audit work to be performed or potential gains in the quality of the audit. Examples of these are the knowledge required by the technical nature of the tasks to be performed, scarce audit resources and limited knowledge of specific areas of audit. An 'expert' could be an IS auditor from the external accounting firm, a management consultant, an IT expert or expert in the area of the audit who has been appointed by top management or by the IS audit team. An expert could be internal or external to an organisation as long as independence and objectivity is maintained.

2. Audit Charter

2.1 Rights of Access to the Work of Other Experts

2.1.1 The IS auditor should verify that, where the work of other experts is relevant to the IS audit objectives, the audit charter or engagement letter specifies the IS auditor's right of access to this work.

3. Planning

3.1 Planning Considerations

3.1.1 When the IS auditor does not have the required skills or other competencies to perform the audit, the IS auditor should seek competent assistance from other experts; however, the IS auditor should have good knowledge of the work performed but not be expected to have a knowledge level equivalent to the experts.

3.1.2 When an IS audit involves using the work of other experts, the IS auditor should consider their activities and their effect on the IS audit objectives whilst planning the IS audit work. The planning process should include:

- Assessing the independence and objectivity of the other experts
- Assessing their professional competence and qualifications
- Obtaining an understanding of their scope of work, approach, timing and quality control processes, including assessing if they exercised due care in creating working papers and retaining evidence of their work
- Determining the level of review required

3.2 Independence and Objectivity

3.2.1 The processes for selection and appointment, the organisational status, the reporting line and the effect of their recommendations on management practices are indicators of the independence and objectivity of other experts.

3.3 Professional Competence

3.3.1 The qualifications, experience, resources and credentials of other experts should all be taken into account in assessing professional competence.

3.4 Scope of Work and Approach

3.4.1 Scope of work and approach ordinarily will be evidenced by the other expert's written audit charter, terms of reference or letter of engagement.

3.5 Level of Review Required

3.5.1 The nature, timing and extent of audit evidence required will depend upon the significance and scope of the other expert's work. The IS auditor's planning process should identify the level of review that is required to provide sufficient reliable, relevant and useful audit evidence to achieve the overall IS audit objectives effectively. The IS auditor should review the other expert's final report, audit programme(s) and audit work papers. The IS auditor should also consider whether supplemental testing of the other expert's work is required.

4. Performance Of Audit Work

4.1 Review of Other Expert's Work Papers

4.1.1 The IS auditor should have access to all work papers created by the expert, supporting documentation and reports of other experts, where such access does not create legal issues.

4.1.2 Where the expert's access to records creates legal issues and, hence, such access is not available, the IS auditor should appropriately determine and conclude the extent of use and reliance on the expert's work.

4.1.3 In reviewing other expert's work papers, the IS auditor should perform sufficient audit work to confirm that the other expert's work was appropriately planned, supervised, documented and reviewed, to consider the appropriateness, sufficiency of the audit evidence provided by them, and to determine the extent of use and reliance on the expert's work. Compliance with relevant professional standards should also be assessed. The IS auditor should assess whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives and document such conclusion.

4.1.4 Based on the assessment of the work of other experts' work papers, the IS auditor should apply additional test procedures to gain sufficient and appropriate audit evidence in circumstances where the work of other experts does not provide sufficient and appropriate audit evidence.

4.1.5 If additional test procedures performed do not provide sufficient and appropriate audit evidence, the IS auditor should provide appropriate audit conclusion and include scope limitation where required.

4.2 Review of Other Expert's Report(s)

4.2.1 The IS auditor should perform sufficient reviews of the other expert's final report(s) to confirm that the scope specified in the audit charter, terms of reference or letter of engagement has been met; that any significant assumptions used by the other experts have been identified; and that the findings and conclusions reported have been agreed upon by management.

4.2.2 It may be appropriate for management to provide their own report on the audited entities, in recognition of their primary responsibility for systems of internal control. In this case, the IS auditor should consider management's and the expert's reports together.

4.2.3 The IS auditor should assess the usefulness and appropriateness of reports issued by the other experts, and should consider any significant findings reported by the other experts. It is the IS auditor's responsibility to assess the effect of the other expert's findings and conclusions on the overall audit objective, and to verify that any additional work required to meet the overall audit objective is completed

4.2.4 If an expert is engaged by another part of the organisation, reliance may be placed on the report of the expert. In some cases this may lessen the need for IS audit coverage even though the IS auditor does not have access to supporting documentation and work papers. The IS auditor should be cautious in providing an opinion on such cases.

4.2.5 The IS auditor's views/comments on the adoptability and relevance of the expert's report should form a part of the IS auditor's report if the expert's report is utilised in forming the IS auditor's opinion.

5. Follow-up Activities

5.1 Implementation of Recommendations

5.1.1 Where appropriate, the IS auditor should consider the extent to which management has implemented any recommendations of other experts. This should include assessing if management has committed to remediation of issues identified by other experts within appropriate time frames and the current status of remediation.

6. Effective Date

6.1 This guideline is effective for all IS audits beginning on or after 1 June 1998. The guideline has been reviewed and updated and is effective 1 March 2008.

2207 Irregularity and Illegal Acts (G9)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S3 (1005) Professional Ethics and Standards states: 'The IS auditor should exercise due professional care, including observance of applicable professional auditing standards'.

1.1.2 Standard S5 (1201) Planning states: 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.3 Standard S6 (1203) Performance of Audit Work states: 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.1.4 Standard S7 (1401) Reporting states: 'The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The audit report should state the scope, objectives, period of coverage, and the nature, timing and extent of the audit work performed. The report should state the findings, conclusions and recommendations and any reservations or qualifications or limitations in scope that the IS auditor has with respect to the audit'.

1.1.5 Standard S9 (1207) Irregularities and Illegal Acts elaborates on requirements and considerations by IS auditors regarding irregularities and illegal acts.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the audit considerations of IS auditors for irregularities and illegal acts, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 The primary COBIT references are:

- PO5 *Manage the IT investment*
- PO7 *Manage IT human resources*
- PO9 *Assess and manage IT risks*
- PO10 *Manage projects*
- AI1 *Identify automated solutions*
- AI5 *Procure IT resources*
- ME2 *Monitor and evaluate internal controls*
- ME3 *Ensure regulatory compliance*
- ME4 *Provide IT governance*

1.2.3 The secondary COBIT references are:

- PO3 *Determine technological direction*
- PO4 *Define the IT processes, organisation and relationships*
- PO8 *Manage quality*
- DS7 *Educate and train users*
- DS10 *Manage problems*
- ME1 *Monitor and evaluate IT performance*

1.2.4 The most relevant COBIT information criteria are:

- Primary: Compliance, confidentiality, integrity and availability
- Secondary: Reliability, efficiency and effectiveness

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to provide guidance to IS auditors to deal with irregular or illegal activities they may come across during the performance of audit assignments.

1.3.2 Standard S9 (1207) Irregularities and Illegal Acts elaborates on requirements and considerations by IS auditors for irregularities and illegal acts. This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the previously identified standards, use professional judgement in its application and be prepared to justify any departure.

2. Definitions

2.1 Non-fraudulent Irregular Activities

2.1.1 Not all irregularities should be considered fraudulent activities. The determination of fraudulent activities depends on the legal definition of fraud in the jurisdiction pertaining to the audit. Irregularities include, but are not limited to, deliberate circumvention of controls with the intent to conceal the perpetuation of fraud, unauthorised use of assets or services, and abetting or helping to conceal these types of activities. Non-fraudulent irregularities may include:

- Intentional violations of established management policy
- Intentional violations of regulatory requirements
- Deliberate misstatements or omissions of information concerning the area under audit or the organisation as a whole
- Gross negligence
- Unintentional illegal acts

2.2 Irregularities and Illegal Acts

2.2.1 Irregularities and illegal acts may include activities such as, but not limited to:

- Fraud, which is any act involving the use of deception to obtain illegal advantage
- Acts that involve non-compliance with laws and regulations, including the failure of IT systems to meet applicable laws and regulations
- Acts that involve non-compliance with the organisation's agreements and contracts with third parties, such as banks, suppliers, vendors, service providers and stakeholders
- Manipulation, falsification, forgery or alteration of records or documents (whether in electronic or paper form)
- Suppression or omission of the effects of transactions from records or documents (whether in electronic or paper form)
- Inappropriate or deliberate leakage of confidential information
- Recording of transactions in financial or other records (whether in electronic or paper form) that lack substance and are known to be false
- Misappropriation and misuse of IS and non-IS assets
- Acts whether intentional or unintentional that violate intellectual property (IP), such as copyright, trademark or patents
- Granting unauthorised access to information and systems
- Errors in financial or other records that arise due to unauthorised access to data and systems

2.2.2 The determination of whether a particular act is illegal generally would be based on the advice of an informed expert qualified to practice law or may have to await final determination by a court of law. The IS auditor should be concerned primarily with the effect or potential effect of the irregular action, irrespective of whether the act is suspected or proven as illegal.

3. Responsibilities

3.1 Responsibilities of Management

3.1.1 It is primarily management's responsibility to prevent and detect irregularities and illegal acts.

3.1.2 Management typically use the following means to obtain reasonable assurance that irregularities and illegal acts are prevented or detected in a timely manner:

- Designing, implementing and maintaining internal control systems to prevent and detect irregularities or illegal acts. Internal controls include transaction review and approval and management review procedures.
- Polices and procedures governing employee conduct
- Compliance validation and monitoring procedures
- Designing, implementing and maintaining suitable systems for the reporting, recording and management of incidents relating to irregularities or illegal acts

3.1.3 Management should disclose to the IS auditor its knowledge of any irregularities or illegal acts and areas affected, whether alleged, suspected or proven, and the action, if any, taken by management.

3.1.4 Where an act of irregularity or illegal nature is alleged, suspected or detected, management should aid the process of investigation and inquiry.

3.2 Responsibilities of IS Auditors

3.2.1 The IS auditor should consider defining in the audit charter or letter of engagement the responsibilities of management and audit with respect to preventing, detecting and reporting irregularities, so that these are clearly understood for all audit work. Where these responsibilities are already documented in the organisation's policy or similar document, the audit charter should include a statement to that effect.

3.2.2 The IS auditor should understand that control mechanisms do not completely eliminate the possibility of irregularities or illegal acts occurring. The IS auditor is responsible for assessing the risk of irregularities or illegal acts occurring, evaluating the impact of identified irregularities, and designing and performing tests that are appropriate for the nature of the audit assignment. The IS auditor can reasonably be expected to detect:

- Irregularities or illegal acts that could have a material effect on either the area under audit or the organisation as a whole
- Weaknesses in internal controls that could result in material irregularities or illegal acts not being prevented or detected

3.2.3 The IS auditor is not professionally responsible for the prevention or detection of irregularities or illegal acts. An audit cannot guarantee that irregularities will be detected. Even when an audit is appropriately planned and performed, irregularities could go undetected, e.g., if there is collusion between employees, collusion between employees and outsiders, or management involvement in the irregularities. The IS auditor should also consider documenting this point in the audit charter or letter of engagement.

3.2.4 Where the IS auditor has specific information about the existence of an irregularity or illegal act, the auditor has an obligation to perform procedures to detect, investigate and report it.

3.2.5 The IS auditor should inform the audit committee (or equivalent) and management when he/she has identified situations where a higher level of risk exists for a potential irregularity or illegal act, even if none is detected.

3.2.6 The IS auditor should be reasonably conversant with the subject to be able to identify risk factors that may contribute to the occurrence of irregular or illegal acts.

3.2.7 IS auditors should ensure that they are independent of the subject during the entire audit assignment.

3.2.8 IS auditors are required to refer to standard S9 (1207) Irregularities and Illegal Acts for a detailed discussion on IS auditors' responsibilities.

4. Risk Assessment

4.1 Planning the Risk Assessment

4.1.1 The IS auditor should assess the risk of occurrence of irregularities or illegal acts connected with the area under audit following the use of the appropriate methodology. In preparing this assessment, the IS auditor should consider factors such as:

- Organisational characteristics, e.g., corporate ethics, organisational structure, adequacy of supervision, compensation and reward structures, the extent of corporate performance pressures, organisation direction
- The history of the organisation, past occurrences of irregularities, and the activities subsequently taken to mitigate or minimise the findings related to irregularities
- Recent changes in management, operations or IS systems and the organisation's current strategic direction
- Impacts resulting from new strategic partnerships
- The types of assets held, or services offered, and their susceptibility to irregularities
- Evaluation of the strength of relevant controls and vulnerabilities to circumvent or bypass established controls
- Applicable regulatory or legal requirements
- Internal policies such as a whistle-blower policy, insider trading policy, and employee and management code of ethics
- Stakeholder relations and financial markets
- Human resources capabilities
- Confidentiality and integrity of market-critical information
- The history of audit findings from previous audits
- The industry and competitive environment in which the organisation operates
- Findings of reviews carried out outside the scope of the audit, such as findings from consultants, quality assurance teams or specific management investigations
- Findings that have arisen during the day-to-day course of business
- Process documentation and a quality management system
- The technical sophistication and complexity of the information system(s) supporting the area under audit
- Existence of in-house developed/maintained application systems, compared with packaged software, for core business systems
- The effect of employee dissatisfaction
- Potential layoffs, outsourcing, divestiture or restructuring
- The existence of assets that are easily susceptible to misappropriation
- Poor organisational financial and/or operational performance
- Management's attitude with regard to ethics
- Irregularities and illegal acts that are common to a particular industry or have occurred in similar organisations

4.1.2 The risk assessment should take into consideration only those factors that are relevant to the organisation and the subject of the engagement, including risk factors relating to:

- Irregularities or illegal acts that affect the financial accounting records
- Irregularities or illegal acts that do not effect the financial records, but affect the organisation
- Other irregularities or illegal acts that relate to the sufficiency of the organisation's controls

4.1.3 As part of the planning process and performance of the risk assessment, the IS auditor should inquire of management with regard to such things as:

- Their understanding regarding the level of risk of irregularities and illegal acts in the organisation
- Whether they have knowledge of irregularities and illegal acts that have or could have occurred against or within the organisation
- How the risk of irregularities or illegal acts is monitored or managed
- What processes are in place to communicate to appropriate stakeholders about the existence of risk of irregularities or illegal acts
- Applicable national and regional laws in the jurisdiction the company operates and extent of coordination of the legal department with the risk committee and audit committee

5. Planning of Audit Work

5.1 Planning the Engagement

5.1.1 While the IS auditor has no explicit responsibility to detect or prevent illegal acts or irregularities, the IS auditor should design the procedures to detect illegal acts or irregularities based on the assessed level of risk that they could occur.

5.1.2 When planning the engagement, the IS auditor should obtain an understanding of such things as:

- A basic understanding of the organisation's operations and objectives
- The internal control environment
- The policies and procedures governing employee conduct
- Compliance validation and monitoring procedures
- The legal and regulatory environment in which the organisation operates
- The mechanism that the organisation uses to obtain, monitor and ensure compliance with the laws and regulations that affect the organisation

5.2 Engagement Procedure

5.2.1 The IS auditor should design procedures for the engagement that take into account the level of riskfor irregularities and illegal acts that have been identified.

5.2.2 The results of the risk assessment and other procedures performed during planning should be used to determine the nature, extent and timing of the procedures performed during an engagement.

5.2.3. The IS auditor should inquire of IT and user management (as appropriate) concerning compliance with laws and regulations.

5.2.4. The IS auditor should use the results of the risk assessment, to determine the nature, timing and extent of the testing required to obtain sufficient audit evidence of reasonable assurance that:

- Irregularities that could have a material effect on the area under audit, or on the organisation as a whole, are identified
- Control weaknesses that would fail to prevent or detect material irregularities are identified
- All significant deficiencies in the design or operation of internal controls that could potentially affect the issuer's ability to record, process, summarise and report business data are identified

5.3 Evaluating the Results of Engagement Procedures

5.3.1 The IS auditor should review the results of engagement procedures to determine whether indications of irregularities or illegal acts may have occurred.

5.3.2 When this evaluation is performed, risk factors identified in section 4 should be reviewed against the actual procedures performed to provide reasonable assurance that all identified risks have been addressed.

5.3.3 The evaluation should also include an assessment of the results of the procedures to determine if undocumented risk factors exist.

6. Performance of Audit Work

6.1 Responding to Possible Illegal Acts

6.1.1 During an engagement, indications that the existence of irregularities or illegal acts may come to the attention of the IS auditor. If indications of an illegal act are identified, the IS auditor should consider the potential effect on the subject matter of the engagement, the report and the organisation.

6.1.2 When the IS auditor becomes aware of information concerning a possible illegal act, the IS auditor should consider taking the following steps:

- Obtain an understanding of the nature of the act.
- Understand the circumstances in which it occurred.
- Obtain sufficient supportive information to evaluate the effect of the irregularity or illegal act.
- Perform additional procedures to determine the effect of the irregularity or illegal act and whether additional acts exist.

6.1.3 The IS auditor should work with appropriate personnel in the organisation (such as organizational security personnel), including management (at an appropriate level above those involved, if possible), to determine whether an irregularity or illegal act has occurred and its effect.

6.1.4 When an irregularity involves a member of management, the IS auditor should reconsider the reliability of representations made by management. As stated previously, typically, the IS auditor should work with an appropriate level of management above the one associated with the irregularity or illegal act.

6.1.5 Unless circumstances clearly indicate otherwise, the IS auditor should assume that an irregularity or illegal act is not an isolated occurrence.

6.1.6 The IS auditor should also review applicable portions of the organisation's internal controls to determine why they failed to prevent or detect the occurrence of an irregularity or illegal act.

6.1.7 The IS auditor should reconsider the prior evaluation of the sufficiency, operation and effectiveness of the organisation's internal controls.

6.1.8 When the IS auditor has identified situations where an irregularity or illegal act exists (whether potential or in fact), the IS auditor should modify the procedures performed to confirm or resolve the issue identified during the engagement's performance. The extent of such modifications or additional procedures depends on the IS auditor's judgement as to the:
- Type of irregularity or illegal act that may have occurred
- Perceived risk of its occurrence
- Potential effect on the organisation, including such things as financial effects and the organisation's reputation
- Likelihood of the recurrence of similar irregularities or illegal acts
- Possibility that management may have knowledge of, or be involved with, the irregularity or illegal act
- Actions, if any, that the governing body and/or management is taking
- Possibility that non-compliance with laws and regulations has occurred unintentionally
- Likelihood that a material fine or other sanctions, e.g., the revocation of an essential licence, may be imposed as a result of non-compliance.
- Effect on the public interest that may result from the irregularity

6.2 Effect of Finding Irregularities

6.2.1 If irregularities have been detected, the IS auditor should assess the effect of these activities on the audit objectives and on the reliability of audit evidence collected. In addition, the IS auditor should consider whether to continue the audit when:
- The effect of irregularities appears to be so significant that sufficient, reliable audit evidence cannot be obtained
- Audit evidence suggests that management, or employees who have a significant role in the issuer's internal controls, have participated in or condoned irregularities

6.3 Effect of Finding Indicators of Irregularities

6.3.1 If the audit evidence indicates that irregularities could have occurred, the IS auditor should:
- Recommend to management that the matter be investigated in detail or the appropriate actions taken. If the IS auditor suspects that management is involved in the irregularity, he/she should identify the appropriate responsible figure in the organisation to whom these conclusions should be reported. If reporting internally proves impossible, the IS auditor should consider consulting the audit committee and legal counsel about the advisability and risks of reporting the findings outside the organisation.
- Perform adequate actions to support the audit findings, conclusions and recommendations

6.4 Legal Considerations

6.4.1 If audit evidence indicates that an irregularity could involve an illegal act, the IS auditor should consider seeking legal advice directly or recommending that management seek legal advice. The IS auditor may want to define responsibility for legal costs in the audit charter or letter of engagement.

7. Reporting

7.1 Internal Reporting

7.1.1 The detection of irregularities should be communicated to appropriate persons in the organisation in a timely manner. The notification should be directed to a level of management above that at which the irregularities are suspected to have occurred. In addition, irregularities should be reported to the board of directors, audit committee of the board, or equivalent body, except for matters that are clearly insignificant in terms of both financial effect and indications of control weaknesses. If the IS auditor suspects that all levels of management are involved, then the findings should be confidentially reported to governing bodies of the organisation, such as the board of directors/ governors, trustees or audit committee, according to the local applicable regulations and laws.

7.1.2 The IS auditor should use professional judgement when reporting an irregularity or illegal act. The IS auditor should discuss the findings and the nature, timing and extent of any further procedures to be performed with an appropriate level of management that is at least one level above the persons who appear to be involved. In these circumstances, it is particularly important that the IS auditor maintains independence. In determining the appropriate persons to whom to report an irregularity or illegal act, the IS auditor should consider all relevant circumstances, including the possibility of senior management involvement.

7.1.3 The internal distribution of reports of irregularities should be considered carefully. The occurrence and effect of irregularities is a sensitive issue and reporting them carries its own risks, including:
- Further abuse of the control weaknesses as a result of publishing details of them
- Loss of customers, suppliers and investors when disclosure (authorised or unauthorised) occurs outside the organisation
- Loss of key staff and management, including those not involved in the irregularity, as confidence in management and the future of the organisation falls

7.1.4 The IS auditor should consider reporting the irregularity separately from any other audit issues if this would assist in controlling distribution of the report.

7.1.5 The IS auditor's report should include:
- Critical policies and practices adopted by the organisation
- If any deviations from generally accepted standards, management's reason for such deviation and the auditor's opinions on such deviations

7.1.6 The IS auditor should seek to avoid alerting any person who may be implicated or involved in the irregularity or illegal act, to reduce the potential for those individuals to destroy or suppress evidence.

7.2 External Reporting

7.2.1 External reporting may be a legal or regulatory obligation. The obligation may apply to the management of the organisation, or the individuals involved in detecting the irregularities, or both. Not withstanding an organisation's responsibility to report an illegal act or irregularity, the IS auditor's duty of confidentiality to the organisation precludes reporting any potential or identified irregularities or illegal acts. However, in certain circumstances, the IS auditor may be required to disclose an irregularity or illegal act. These include such things as:

- Compliance with legal or regulatory requirements
- External auditor requests
- Subpoena or court order
- Funding agency or government agency in accordance with requirements for the audits of entities that receive governmental financial assistance

7.2.2 Where external reporting is required, the report should be approved by the appropriate level of audit management prior to external release and should also be reviewed with auditee management in advance, unless the applicable regulations or specific circumstances of the audit prevent this. Examples of specific circumstances that may prevent obtaining auditee management's agreement include:

- Auditee management's active involvement in the irregularity
- Auditee management's passive acquiescence to the irregularity

7.2.3 If auditee management does not agree to the external release of the report, and external reporting is a statutory or a regulatory obligation, then the IS auditor should consider consulting the audit committee and legal counsel about the advisability and risks of reporting the findings outside the organisation. In some jurisdictions, the IS auditor may be protected by qualified privilege. Even in situations where IS auditor's are protected by privilege, IS auditors should seek legal advice and counsel prior to making this type of disclosure to ensure that they are in fact protected by this privilege.

7.2.4 The IS auditor, with the approval of audit management, should submit the report to appropriate regulators on a timely basis. If the organisation fails to disclose a known irregularity or illegal act or requires the IS auditor to suppress these findings, the IS auditor should seek legal advice and counsel.

7.2.5 Where the IS auditor is aware that management is required to report fraudulent activities to an outside organisation, the IS auditor should formally advise management of this responsibility.

7.2.6 If an irregularity has been detected by an IS auditor who is not part of the external audit team, then the IS auditor should consider submitting the report to the external auditors in a timely manner.

7.3 Restriction of Audit Scope

7.3.1 Where the audit scope has been restricted, the IS auditor should include an explanation of the nature and effect of this restriction in the audit report. Such a restriction may occur if:

- The IS auditor has been unable to carry out the further work considered necessary to fulfil the original audit objectives and support the audit conclusions, e.g., because of unreliable audit evidence, lack of resource or restrictions placed on the audit activities by management
- Management has not carried out the investigations recommended by the IS auditor

8 Effective Date

8.1 This guideline is effective for all IS audits beginning on or after 1 March 2000. This guideline has been reviewed and updated, combined with and replaces G19 Irregularities and Illegal Acts, effective 1 September 2008.

2208 Audit Sampling (G10)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S6 (1203) Performance of Audit Work states: 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT, applicable to the scope of the particular audit, is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the audit sampling requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 ME2 *Monitor and evaluate internal control* satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws, regulations and contracts by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.2.3 ME3 *Ensure regulatory compliance* satisfies the business requirement for IT of compliance with laws and regulations by focusing on identifying all applicable laws and regulations and the corresponding level of IT compliance and optimising IT processes to reduce the risk of non-compliance.

1.2.4 The primary references are:

- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*
- AI6 *Manage changes*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure regulatory compliance*

1.2.5 The information criteria most relevant are:

- Primary: Effectiveness, integrity, reliability and compliance
- Secondary: Confidentiality, efficiency and availability

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to provide guidance to the IS auditor to design and select an audit sample and evaluate sample results. Appropriate sampling and evaluation will meet the requirements of 'sufficient, reliable, relevant and useful evidence' and 'supported by appropriate analysis'.

1.3.2 The IS auditor should consider selection techniques that result in a statistically based representative sample for performing compliance or substantive testing.

1.3.3 Examples of compliance testing of controls, where sampling could be considered, include user access rights, program change control procedures, procedures documentation, program documentation, follow-up on exceptions, review of logs and software licences audits.

1.3.4 Examples of substantive tests, where sampling could be considered, include reperformance of a complex calculation (e.g., interest) on a sample of accounts, sample of transactions to vouch to supporting documentation, etc.

1.3.5 This guideline provides guidance in applying IS Auditing Standards. The IS auditor should consider it in determining how to achieve implementation of standard S6 (1203) , use professional judgement in its application and be prepared to justify any departure.

1.3.6 Other useful references on audit sampling include the International Standard on Auditing #530 Audit Sampling and Other Selective Testing Procedures, issued by the International Federation of Accountants (IFAC).

2. Performance of Audit Work

2.1 Audit Sampling

2.1.1 When using either statistical or non-statistical sampling methods, the IS auditor should design and select an audit sample, perform audit procedures, and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence.

2.1.2 In forming an audit opinion, IS auditors frequently do not examine all of the information available as it may be impractical and valid conclusions can be reached using audit sampling.

2.1.3 Audit sampling is defined as the application of audit procedures to less than 100 percent of the population to enable the IS auditor to evaluate audit evidence about some characteristic of the items selected to form or assist in forming a conclusion concerning the population.

2.1.4 Statistical sampling involves the use of techniques from which mathematically constructed conclusions regarding the population can be drawn.

2.1.5 Non-statistical sampling is not statistically based, and results should not be extrapolated over the population as the sample is unlikely to be representative of the population.

2.2 Design of the Sample

2.2.1 When designing the size and structure of an audit sample, IS auditors should consider the specific audit objectives, the nature of the population, and the sampling and selection methods.

2.2.2 The IS auditor should consider the need to involve appropriate specialists in the design and analysis of samples.

2.2.3 The sampling unit depends on the purpose of the sample. For compliance testing of controls, attribute sampling is typically used, where the sampling unit is an event or transaction (e.g., a control such as an authorisation on an invoice). For substantive testing, variable or estimation sampling is frequently used where the sampling unit is often monetary.

2.2.4 The IS auditor should consider the specific audit objectives to be achieved and the audit procedures that are most likely to achieve those objectives. In addition, when audit sampling is appropriate, consideration should be given to the nature of the audit evidence sought and possible error conditions.

2.2.5 The population is the entire set of data from which the IS auditor wishes to sample to reach a conclusion on the population. Therefore, the population from which the sample is drawn has to be appropriate and verified as complete for the specific audit objective.

2.2.6 To assist in the efficient and effective design of the sample, stratification may be appropriate. Stratification is the process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum.

2.2.7 When determining sample size, the IS auditor should consider the sampling risk, the amount of the error that would be acceptable and the extent to which errors are expected.

2.2.8 Sampling risk arises from the possibility that the IS auditor's conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risk:

- The risk of incorrect acceptance—The risk that material misstatement is assessed as unlikely when, in fact, the population is materially misstated
- The risk of incorrect rejection—The risk that material misstatement is assessed as likely when, in fact, the population is not materially misstated

2.2.9 Sample size is affected by the level of sampling risk that the IS auditor is willing to accept. Sampling risk should also be considered in relation to the audit risk model and its components, inherent risk, control risk, and detection risk.

2.2.10 Tolerable error is the maximum error in the population that IS auditors are willing to accept and still conclude that the audit objective has been achieved. For substantive tests, tolerable error is related to the IS auditor's judgement about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the IS auditor is willing to accept.

2.2.11 If the IS auditor expects errors to be present in the population, a larger sample than when no error is expected ordinarily has to be examined to conclude that the actual error in the population is not greater than the planned tolerable error. Smaller sample sizes are justified when the population is expected to be error free. When determining the expected error in a population, the IS auditor should consider such matters as error levels identified in previous audits, changes in the organisation's procedures, and evidence available from an evaluation of the system of internal control and results from analytical review procedures.

2.3 Selection of the Sample

2.3.1 There are four commonly used sampling methods. Statistical sampling methods are:

- Random sampling—Ensures that all combinations of sampling units in the population have an equal chance of selection
- Systematic sampling—Involves selecting sampling units using a fixed interval between selections, the first interval having a random start. Examples include Monetary Unit Sampling or Value Weighted selection where each individual monetary value (e.g., $1) in the population is given an equal chance of selection. As the individual monetary unit cannot ordinarily be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weights the selection in favour of the larger amounts but still gives every monetary value an equal opportunity for selection. Another example includes selecting every 'nth sampling unit

Nonstatistical sampling methods are:

- Haphazard sampling—The IS auditor selects the sample without following a structured technique, while avoiding any conscious bias or predictability. However, analysis of a haphazard sample should not be relied upon to form a conclusion on the population
- Judgmental sampling—The IS auditor places a bias on the sample (e.g., all sampling units over a certain value, all for a specific type of exception, all negatives, all new users). It should be noted that a judgemental sample is not statistically based and results should not be extrapolated over the population as the sample is unlikely to be representative of the population.

2.3.2 The IS auditor should select sample items in such a way that the sample is expected to be representative of the population regarding the characteristics being tested, i.e., using statistical sampling methods. To maintain audit independence, the IS auditor should ensure that the population is complete and control the selection of the sample.

2.3.3 For a sample to be representative of the population, all sampling units in the population should have an equal or known probability of being selected, i.e., statistical sampling methods.

2.3.4 There are two commonly used selection methods: selection on records and selection on quantitative fields (e.g., monetary units).

For selection on records, common methods are:
- Random sample (statistical sample)
- Haphazard sample (non-statistical)
- Judgemental sample (non-statistical; high probability to lead to a biased conclusion)

For selection on quantitative fields, common methods are:
- Random sample (statistical sample on monetary units)
- Fixed Interval sample (statistical sample using a fixed interval)
- Cell sample (statistical sample using random selection in an interval)

2.4 Documentation

2.4.1 The audit work papers should include sufficient detail to describe clearly the sampling objective and the sampling process used. The work papers should include the source of the population, the sampling method used, sampling parameters (e.g., random start number or method by which random start was obtained, sampling interval), items selected, details of audit tests performed and conclusions reached.

2.5 Evaluation of Sample Results

2.5.1 Having performed, on each sample item, those audit procedures which are appropriate to the particular audit objective, the IS auditor should analyse any possible errors detected in the sample to determine whether they are actually errors and, if appropriate, the nature and cause of the errors. For those that are assessed as errors, the errors should be projected as appropriate to the population, if the sampling method used, is statistically based.

2.5.2 Any possible errors detected in the sample should be reviewed to determine whether they are actually errors. The IS auditor should consider the qualitative aspects of the errors. These include the nature and cause of the error and the possible effect of the error on the other phases of the audit. Errors that are the result of the breakdown of an automated process ordinarily have wider implications for error rates than human error.

2.5.3 When the expected audit evidence regarding a specific sample item cannot be obtained, the IS auditor may be able to obtain sufficient, appropriate audit evidence by performing alternative procedures on the item selected.

2.5.4 The IS auditor should consider projecting the results of the sample to the population with a method of projection consistent with the method used to select the sampling unit. The projection of the sample may involve estimating the probable error in the population and estimating any further error that might not have been detected because of the imprecision of the technique together with the qualitative aspects of any errors found.

2.5.5 The IS auditor should consider whether errors in the population might exceed the tolerable error by comparing the projected population error to the tolerable error, taking into account the results of other audit procedures relevant to the audit objective. When the projected population error exceeds the tolerable error, the IS auditor should reassess the sampling risk and, if that risk is unacceptable, consider extending the audit procedure or performing alternative audit procedures.

3. Effective Date

3.1 This guideline is effective for all IS audits beginning on or after 1 March 2000. The guideline has been reviewed and updated effective 1 August 2008.

Reporting Guidelines

The reporting guidelines are:
2401 Reporting (G20)
2402 Follow-up Activities (G35)

The guidelines are included here in their entirety. For links to the individual standards, visit *www.isaca.org/standard*.

2401 Reporting (G20)

1. Background

1.1 Linkage to ISACA Standards

1.1.1. Standard S7 (1401) Reporting states 'The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The report should identify the organisation, the intended recipients and any restrictions on circulation. The report should state the scope, objectives, period of coverage, and the nature, timing and extent of the audit work performed. The report should state the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IS auditor has with respect to the audit'.

1.2 Definitions

1.2.1. Subject matter or area of activity is the specific information subject to the IT audit and assurance professional's report and related procedures. It can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations.

1.2.2. Attest reporting engagement is an engagement where an IT audit and assurance professional either examines management's assertions regarding a particular subject matter or the subject matter directly. The IT audit and assurance professional's report consists of an opinion on one of the following:

- The subject matter. These reports relate directly to the subject matter itself rather than an assertion. In certain situations management will not be able to make an assertion over the subject of the engagement. An example of this situation is when IT services are outsourced to a third party. Management will not ordinarily be able to make an assertion over the controls for which the third party is responsible. Hence, an IT audit and assurance professional would have to report directly on the subject matter rather than an assertion.
- Management's assertion about the effectiveness of the control procedures
- An examination reporting engagement, where the IT audit and assurance professional issues an opinion on a particular subject matter. These engagements can include reports on controls implemented by management and on their operating effectiveness.

  This guideline is directed towards the first type of opinion. If the terms of reference require the latter types of opinion, the reporting requirements may need to be adapted.

1.2.3. Control objectives are the objectives of management that are used as the framework for developing and implementing controls (control procedures).

1.2.4 Controls or control procedures means those policies and procedures implemented to achieve a related control objective.

1.2.5. Control weakness means a deficiency in the design or operation of a control procedure. Control weaknesses potentially can result in risks relevant to the area of activity not being reduced to an acceptable level (relevant risks are those that threaten achievement of the objectives relevant to the area of activity being examined). Control weaknesses can be material when the design or operation of one or more control procedures does not reduce, to a relatively low level, the risk that misstatements caused by illegal acts or irregularities may occur and not be detected by the related control procedures.

1.2.6. Criteria are the standards and benchmarks used to measure and present the subject matter and against which the IT audit and assurance professional evaluates the subject matter. Criteria should be:

- Objective—Free from bias
- Measurable—Provide for consistent measurement
- Complete—Include all relevant factors to reach a conclusion
- Relevant—Relate to the subject matter

1.2.7. Direct reporting engagement is an engagement where management does not make a written assertion about the effectiveness of their control procedures and the IT audit and assurance professional provides an opinion, such as the effectiveness of the control procedures, about the subject matter directly.

1.2.8. Internal control structure (internal control) is the dynamic, integrated processes affected by the governing body, management and all other staff, and it is designed to provide reasonable assurance regarding the achievement of the following general objectives:

- Effectiveness, efficiency and economy of operations
- Reliability of management
- Compliance with applicable laws, regulations and internal policies

1.2.9 Management's strategies for achieving these general objectives are affected by the design and operation of the following components:

- Control environment
- Information system
- Control procedures

1.3 Need for Guideline

1.3.1 This guideline sets out how the IT audit and assurance professional should comply with ISACA IT Audit and Assurance Standards and COBIT when reporting on an enterprise's information system controls and related control objectives.

2. Introduction

2.1. Purpose of This Guideline

2.1.1 The purpose of this guideline is to provide direction to IT audit and assurance professionals engaged to report on whether control procedures for a specified area of activity are effective to either:

- An enterprise's management at the governing body and/or operational level
- A specified third party, for example a regulator or another auditor

2.1.2 The IT audit and assurance professional may be engaged to report on design effectiveness or operating effectiveness.

3. Assurance

3.1 Types of Services

3.1.1 An IT audit and assurance professional may perform any of the following:

- Audit (direct or attest)
- Review (direct or attest)
- Agreed-upon procedures

3.2 Audit and Review

3.2.1 An audit provides a high, but not absolute, level of assurance about the effectiveness of control procedures. This ordinarily is expressed as reasonable assurance in recognition of the fact that absolute assurance is rarely attainable due to such factors as the need for judgement, the use of testing, the inherent limitations of internal control and because much of the evidence available to the IT audit and assurance professional is persuasive rather than conclusive in nature.

3.2.2 A review provides a moderate level of assurance about the effectiveness of control procedures. The level of assurance provided is less than that provided in an audit because the scope of the work is less extensive than that of an audit, and the nature, timing and extent of the procedures performed do not provide sufficient and appropriate audit evidence to enable the IT audit and assurance professional to express a positive opinion. The objective of a review is to enable the IT audit and assurance professional to state whether, on the basis of procedures, anything has come to the theirattention that causes the IT audit and assurance professional to believe that the control procedures were not effective based on identified criteria (expression of negative assurance).

3.2.3 Both audits and reviews of control procedures involve:

- Planning the engagement
- Evaluating the design effectiveness of control procedures
- Testing the operating effectiveness of the control procedures (the nature, timing and extent of testing will vary as between an audit and a review)
- Forming a conclusion about, and reporting on, the design and operating effectiveness of the control procedures based on the identified criteria:
  – The conclusion for an audit is expressed as a positive expression of opinion and provides a high level of assurance.
  –The conclusion for a review is expressed as a statement of negative assurance and provides only a moderate level of assurance.

3.3 Agreed-upon Procedures

3.3.1 An agreed-upon procedures engagement does not result in the expression of any assurance by the IT audit and assurance professional. The IT audit and assurance professional is engaged to carry out specific procedures to meet the information needs of those parties who have agreed to the procedures to be performed. The IT audit and assurance professional issues a report of factual findings to those parties that have agreed to the procedures. The recipients form their own conclusions from this report because the IT audit and assurance professional has not determined the nature, timing and extent of procedures to be able to express any assurance. The report is restricted to those parties (e.g.,, a regulatory body) that have agreed to the procedures to be performed, since others are not aware of the reasons for the procedures and may misinterpret the result.

3.4 Agreed-upon Procedures Reporting

3.4.1 The report on agreed-upon procedures should be in the form of procedures and findings. The report should contain the following elements:

- A title that includes the word independent
- Identification of the specified parties
- Identification of the subject matter (or the written assertion related thereto) and the type of engagement
- Identification of the responsible party
- A statement that the subject matter is the responsibility of the responsible party
- A statement that the procedures performed were those agreed to by the parties identified in the report
- A statement that the sufficiency of the procedures is solely the responsibility of the specified parties and a disclaimer of responsibility for the sufficiency of those procedures

- A list of the procedures performed (or reference thereto) and related findings
- A statement that the IT audit and assurance professional was not engaged in and did not conduct an examination of the subject matter
- A statement that if the IT audit and assurance professional had performed additional procedures, other matters might have come to the IT audit and assurance professional's attention and would have been reported
- A statement of restrictions on the use of the report because it is intended to be used solely by the specified parties

3.5 Engagement Mandate

3.5.1 Where an engagement is to be undertaken to meet a regulatory or similarly imposed requirement, it is important that the IT audit and assurance professional be satisfied that the type of engagement is clear from the relevant legislation or other source of the engagement mandate. If there is any uncertainty, it is recommended that the IT audit and assurance professional and/or appointing party communicate with the relevant regulator or other party responsible for establishing or regulating the requirement and agree with the engagement type and the assurance to be provided.

3.5.2 An IT audit and assurance professional who, before the completion of an engagement, is requested to change the engagement from an audit to a review or agreed-upon procedures engagement needs to consider the appropriateness of doing so and cannot agree to a change where there is no reasonable justification for the change. For example, a change is not appropriate to avoid a modified report.

4. IS Audit Opinion

4.1 Limitations

4.1.1 The IT audit and assurance professional's opinion is based on the procedures determined to be necessary for the collection of sufficient and appropriate evidence—that evidence being persuasive rather than conclusive in nature. The assurance provided by an IT audit and assurance professional on the effectiveness of internal controls is, however, restricted because of the nature of internal controls and the inherent limitations of any set of internal controls and their operations. These limitations include:

- Management's usual requirement that the cost of an internal control does not exceed the expected benefits to be derived
- Most internal controls tend to be directed at routine rather than non-routine transactions/events
- The potential for human error due to carelessness, distraction or fatigue, misunderstanding of instructions, and mistakes in judgement
- The possibility of circumvention of internal controls through the collusion of employees with one another or with parties outside the enterprise
- The possibility that a person responsible for exercising an internal control could abuse that responsibility, e.g., a member of management overriding a control procedure
- The possibility that management may not be subject to the same internal controls applicable to other personnel
- The possibility that internal controls may become inadequate due to changes in conditions and that compliance with procedures may deteriorate

4.1.2 Custom, culture and the governance of (corporate and IT) systems may inhibit irregularities by management, but they are not infallible deterrents. An effective control environment may help mitigate the probability of such irregularities. Control environment factors such as an effective governing body, audit committee and internal audit function may constrain improper conduct by management. Alternatively, an ineffective control environment may negate the effectiveness of control procedures within the internal control structure. For example, although an enterprise has adequate IT control procedures relating to compliance with environmental regulations, management may have a strong bias to suppress information about any detected breaches that would reflect adversely on the enterprise's public image. The effectiveness or relevance of internal controls might also be affected by factors such as a change in ownership or control, changes in management or other personnel, or developments in the enterprise's market or industry.

4.2 Subsequent Events

4.2.1 Events sometimes occur, subsequent to the point in time or period of time of the subject matter being tested but prior to the date of the IT audit and assurance professional's report, that have a material affect on the subject matter and that, therefore, require adjustment or disclosure in the presentation of the subject matter or assertion. These occurrences are referred to as subsequent events. In performing an attest engagement, IT audit and assurance professionals should consider information about subsequent events that come to their attention. However, IT audit and assurance professionals have no responsibility to detect subsequent events.

4.2.2 IT audit and assurance professionals should inquire of management as to whether they are aware of any subsequent events, through to the date of IT audit and assurance professional's report, that would have a material effect on the subject matter or assertion.

4.3 Conclusions and Reporting

4.3.1 The IT audit and assurance professional should conclude whether sufficient appropriate evidence has been obtained to support the conclusions in the report. In developing the report, all relevant evidence obtained should be considered, regardless of whether it appears to corroborate or contradict the subject matter information. Where there is an opinion, it should be supported by the results of the control procedures based on the identified criteria.

4.3.2 An IT audit and assurance professional's report about the effectiveness of control procedures should include the following elements:
- Title
- Addressee
- Description of the scope of the audit, the name of the entity or component of the entity to which the subject matter relates, including:
  –Identification or description of the area of activity
  –Criteria used as a basis for the IS audit and assurance professional's conclusion
  –The point in time or period of time to which the work, evaluation or measure of the subject matter relates
  –A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management
- Where the engagement is an attest engagement, a statement identifying the source of management's representation about the effectiveness of control procedures
- A statement that the IT audit and assurance professional has conducted the engagement to express an opinion on the effectiveness of control procedures
- Identification of the purpose for which the IT audit and assurance professional's report has been prepared and of those entitled to rely on it, and a disclaimer of liability for its use for any other purpose or by any other person
- Description of the criteria or disclosure of the source of the criteria
- Statement that the audit has been conducted in accordance with ISACA IT Audit and Assurance Standards or other applicable professional standards
- Further explanatory details about the variables that affect the assurance provided and other information as appropriate
- Where appropriate, a separate report should include recommendations for corrective action and include management's response
- A paragraph stating that because of the inherent limitations of any internal control, misstatements due to errors or fraud may occur and go undetected. In addition, the paragraph should state that projections of any evaluation of internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the level of compliance with the policies or procedures may deteriorate. An audit is not designed to detect all weaknesses in control procedures as it is not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis. When the IT audit and assurance professional's opinion is qualified, a paragraph describing the qualification should be included.
- An expression of opinion about whether, in all material respects, the design and operation of control procedures in relation to the area of activity were effective
- IT audit and assurance professional's signature
- IT audit and assurance professional's address
- Date of the IT audit and assurance professional's report. In most instances, the dating of the report is based upon applicable professional standards. In other instances, the date of the report should be based on the conclusion of the fieldwork

4.3.3 In a direct reporting engagement, the IT audit and assurance professional reports directly on the subject matter rather than on an assertion. The report should make reference only to the subject of the engagement and should not contain any reference to management's assertion on the subject matter.

4.3.4 Where the IT audit and assurance professional undertakes a review engagement, the report indicates that the conclusion relates to design and operating effectiveness, and that the IT audit and assurance professional's work in relation to operating effectiveness was limited primarily to inquiries, inspection, observation and minimal testing of the operation of the internal controls. The report includes a statement that an audit has not been performed, that the procedures undertaken provide less assurance than an audit and that an audit opinion is not expressed. The expression of negative assurance states that nothing has come to the IT audit and assurance professional's attention that was a cause to believe the enterprise's control procedures were, in any material respect, ineffective in relation to the area of activity, based on the identified criteria.

4.3.5 During the course of the engagement the IT audit and assurance professional may become aware of control weaknesses. The IT audit and assurance professional should report to an appropriate level of management in a timely manner any identified control weaknesses. The engagement procedures are designed to gather sufficient and appropriate evidence to form a conclusion in accordance with the terms of the engagement. In the absence of a specific requirement in the terms of engagement, the IT audit and assurance professional does not have a responsibility to design procedures to identify matters that may be appropriate to report to management.

5. Effective Date

5.1 This guideline is effective for all IT audits beginning on or after 16 September 2010.

2402 Follow-up Activities (G35)

1. Background

1.1 Linkage to Standards

1.1.1 Standard S8 (1402) Follow-up Activities states, "After the reporting of findings and recommendations, the IS auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner".

1.2 Linkage to COBIT

1.2.1 High-level control objective M3 (*Obtain independent assurance) states*, "…obtaining independent assurance to increase confidence and trust amongst the organisations, customers and third-party providers".

1.2.2 High-level control objective M4 (*Provide for independent audit*) states, "…providing for independent audit to increase confidence levels and benefit from best practice advice".

1.2.3 Detailed control objective M4.8 (*Follow-up activities*) states, "Resolution of audit comments rests with management. Auditors should request and evaluate appropriate information on previous findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner".

1.3 COBIT Reference

1.3.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the requirement, the processes in COBIT likely to be the most relevant selected and adapted are classified below as primary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- M3—*Obtain independent assurance*
- M4—*Provide for independent audit*

1.3.3 The information criteria most relevant to competence are:

- Primary: effectiveness, efficiency, confidentiality, integrity and compliance
- Secondary: availability and reliability

1.4 Purpose of the Guideline

1.4.1 The purpose of this guideline is to provide direction to IS auditors engaged in following up on recommendations and audit comments made in reports.

1.4.2 This guideline provides guidance in applying IS Auditing Standard S8 (1402) Follow-up Activities.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

2. Follow-up Activities

2.1 Definition

2.1.1 Follow-up activities by IS auditors can be defined "as a process by which they determine the adequacy, effectiveness and timeliness of actions taken by management on reported engagement observations and recommendations, including those made by external auditors and others."[1]

2.1.2 A follow-up process should be established to help provide reasonable assurance that each review conducted by the IS auditors provides optimal benefit to the organisation by requiring that agreed-upon outcomes arising from reviews are implemented in accordance with management undertakings or that management recognises and acknowledges the risks inherent in delaying or not implementing proposed outcomes.

2.2 Management's Proposed Actions

2.2.1 As part of the IS auditor's discussions with the engagement organisation, the IS auditor should obtain agreement on the results of the engagement and on a plan of action to improve operations, as needed.

2.2.2 Management should provide an implementation/action date when each proposed action is to be completed.

2.2.3 When management's proposed actions to implement or otherwise address reported recommendations and audit comments have been discussed with or provided to the IS auditor, these actions should be recorded as a management response in the final report with a committed implementation date.

2.2.4 If the IS auditor and engagement organisation disagree about a particular recommendation or audit comment, the engagement communications may state both positions and the reasons for the disagreement. The organisation's written comments may be included as an appendix to the engagement report. Alternatively, the organisation's views may be presented in the body of the report or in a cover letter. Senior management (or the audit committee if one exists) should then make a decision as to which point of view they support. If senior management (or the audit committee) supports the view of the organisation in a particular case, the IS auditor need not follow-up with that particular recommendation, unless it is considered that the significance and level of effect of the observation has changed due to a change(s) in the IS environment (refer to section 2.4.3).

[1] Institute of Internal Auditors (IIA), "Practice Advisory 2500.A1-1," 2002

2.2.5 During some reviews, such as pre-implementation application system reviews, findings may be reported to the project team and/or management on an ongoing basis often in the form of issue statements. In these cases, actions to resolve issues raised should be monitored on an ongoing basis. If issue statement recommendations have been implemented, then "completed" or "implemented" can be recorded against the recommendation in the final report. "Completed" or "implemented" recommendations should be reported.

2.3 Follow-up Procedures

2.3.1 Procedures for follow-up activities should be established and should include:
- The recording of a time frame within which management should respond to agreed-upon recommendations
- An evaluation of management's response
- A verification of the response, if thought appropriate (refer to section 2.7)
- Follow-up work, if thought appropriate
- A communications procedure that escalates outstanding and unsatisfactory responses/actions to the appropriate levels of management
- A process for providing reasonable assurance of management's assumption of associated risks, in the event that remedial action is delayed or not proposed to be implemented

2.3.2 An automated tracking system or database can assist in the carrying out of follow-up activities.

2.3.3 Factors that should be considered in determining appropriate follow-up procedures are:
- Any changes in the IS environment that may affect the significance of a reported observation
- The significance of the reported finding or recommendation
- The effect that may result should the corrective action fail
- The degree of effort and cost needed to correct the reported issue
- The complexity of the corrective action
- The time period involved

2.3.4 If the IS auditor is working in an internal audit environment, responsibility for follow-up should be defined in the internal audit activity's written charter.

2.4 Timing and Scheduling of Follow-up Activities

2.4.1 The nature, timing and extent of the follow-up activities should take into account the significance of the reported finding and the effect if corrective action is not taken. The timing of IS audit follow-up activities in relation to the original reporting is a matter of professional judgement dependent on a number of considerations, such as the nature or magnitude of associated risks and costs to the organisation.

2.4.2 Agreed-upon outcomes relating to high-risk issues should be followed up soon after the due date for action and may be monitored progressively.

2.4.3 Because they are an integral part of the IS audit process, follow-up activities should be scheduled, along with the other steps necessary to perform each review. Specific follow-up activities and the timing of such activities may be influenced by the results of the review and may be established in consultation with line management.

2.4.4 In a particular report, the implementation of all the management responses may be followed up together even though the implementation dates committed to by management may be different. Another approach is to follow up individual management responses according to the due date agreed to with management.

2.5 Deferring Follow-up Activities

2.5.1 The IS auditor is responsible for scheduling follow-up activities as part of developing engagement work schedules. The scheduling of follow-ups should be based on the risk and exposure involved, as well as the degree of difficulty and the significance of timing in implementing corrective action.

2.5.2 There may also be instances where the IS auditor judges that management's oral or written response shows that action already taken is sufficient when weighed against the relative importance of the engagement observation or recommendation. On such occasions, actual follow-up verification activities may be performed as part of the next engagement that deals with the relevant system or issue.

2.6 The Form of Follow-up Responses

2.6.1 The most effective way to receive follow-up responses from management is in writing, as this helps to reinforce and confirm management responsibility for follow-up action and progress achieved. Also, written responses ensure an accurate record of actions, responsibilities and current status. Oral responses may also be received and recorded by the IS auditor and where possible approved by management. Proof of action or implementation of recommendations may also be provided with the response.

2.6.2 The IS auditor may request and/or receive periodic updates from management to evaluate the progress management has made to carry out its agreed-upon actions, particularly in relation to high-risk issues and remedial actions with long lead times.

2.7 Nature and Extent of Follow-up Activities

2.7.1 Normally, the IS auditor will request follow-up status from the organisation soon after the proposed implementation date of some or all of the agreed-upon actions has passed. This may involve reformatting the final report to give the organisation an area in the report to document the details of actions taken to implement recommendations.

2.7.2 The organisation will normally be given a time frame within which to respond with details of actions taken to implement recommendations.

2.7.3 Management's response detailing the actions taken should be evaluated, if possible, by the IS auditor who performed the original review. Wherever possible, audit evidence of action taken should be obtained. For example, procedures may have been documented or a certain management report produced.

2.7.4 Where management provides information on actions taken to implement recommendations and the IS auditor has doubts about the information provided or the effectiveness of the action taken, appropriate testing or other audit procedures should be undertaken to confirm the true position or status prior to concluding follow-up activities.

2.7.5 As a part of the follow-up activities, the IS auditor should evaluate whether unimplemented findings are still relevant or have a greater significance. The IS auditor may decide that the implementation of a particular recommendation is no longer appropriate. This could occur where application systems have changed, where compensating controls have been implemented, or where business objectives or priorities have changed in such a way as to effectively remove or significantly reduce the original risk. In the same way, a change in the IS environment may increase the significance of the effect of a previous observation and the need for its resolution.

2.7.6 A follow-up engagement may have to be scheduled to verify the implementation of critical/important actions.

2.7.7 The IS auditor's opinion on unsatisfactory management responses or action should be communicated to the appropriate level of management.

2.8 Acceptance of Risks by Management

2.8.1 Management is responsible for deciding the appropriate action to be taken in response to reported engagement observations and recommendations. The IS auditor is responsible for assessing such management action for appropriateness and the timely resolution of the matters reported as engagement observations and recommendations.

2.8.2 Senior management may decide to accept the risk of not correcting the reported condition because of cost or other considerations. The board (or the audit committee if one exists) should be informed of senior management's decision on all significant engagement observations and recommendations.

2.8.3 When the IS auditor believes that the organisation has accepted a level of residual risk that is inappropriate for the organisation, the IS auditor should discuss the matter with internal audit and senior management. If the IS auditor is not in agreement with the decision regarding residual risk, the IS auditor and senior management should report the matter to the board (or the audit committee, if one exists) for resolution.

2.9 External Audit Follow-up by an Internal IS Auditor

2.9.1 Follow-up responsibilities for ongoing internal audit activities should be assigned in the audit charter of the internal IS audit function, and for other audit assignments in the engagement letters.

2.9.2 Depending on the scope and terms of the engagement and in accordance with the relevant IS Auditing Standards, external IS auditors may rely on an internal IS audit function to follow-up on their agreed-upon recommendations.

3. Consulting

3.1 Consulting Type Engagements

3.1.1 Consulting type engagements or services can be defined as "advisory and related client service activities, the nature and scope of which are agreed upon with the client and which are intended to add value and improve an organisation's operations. Examples include counsel, advice, facilitation, process design and training."2 The nature and scope of the engagement should be agreed before the engagement begins.

3.1.2 The IS auditor should monitor the results of consulting engagements to the extent agreed upon with the organisation. Varying types of monitoring may be appropriate for differing types of consulting engagements. The monitoring effort may depend on factors, such as, management's explicit interest in the engagement outcomes or the IS auditor's assessment of the project's risks and/or potential additional value to the organisation identified by the engagement.

4. Reporting

4.1 Reporting of Follow-up Activities

4.1.1 A report on the status of agreed remedial actions arising from IS audit reports, including agreed recommendations not implemented, should be presented to the audit committee, if one has been established, or alternatively to the appropriate level of organisation management.

4.1.2 If during a subsequent engagement, the IS auditor finds that the action that management had purported as "implemented" had in fact not been implemented, this should be communicated to senior management and the audit committee if one is in place.

4.1.3 When all the agreed remedial actions have been implemented, a report detailing all the implemented/completed actions can be forwarded to senior management (or the audit committee, if one exists).

5. Effective Date

5.1 This guideline is effective for all information systems audits beginning 1 March 2006. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

3. IS Audit and Assurance Tools and Techniques

Tools and techniques provide additional examples for IS audit and assurance professionals. This section may include references to other relevant and reliable sources as well as ISACA:

- White papers, *www.isaca.org/whitepapers* (complimentary PDF files)
- Audit/assurance programs. *www.isaca.org/auditprograms* (complimentary Word files for ISACA members)
- COBIT 5 family of products, *www.isaca.org/cobit*
- Technical and Risk Management Reference series, *www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/Pages/Reference-Series.aspx* (available in the ISACA Bookstore)
- Journal IT Audit Basics columns, *www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/IT-Audit-Basics/Pages/IT-Audit-Basics-Articles.*aspx (complimentary access)

All ISACA research deliverables are listed on page *www.isaca.org/Knowledge-Center/Research/Pages/All-Deliverables.aspx*.

For additional information about obtaining a particular ISACA publication, visit *www.isaca.org/bookstore or e-mail bookstore@isaca.org*.

Comment Submission Form

We are interested in your reaction to ITAF and any additions/revisions you might suggest. Please provide detailed information about your suggestion as well as your rationale for the revision. Submit your comments to the attention of the director of professional standards development via fax at +1.847.253.1443, e-mail to *standards@isaca.org* or mail to ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA.

Name: _____

Organisation: _____

Country: _____ E-mail address: _____

Section: _____

Suggested revision: _____

_____

_____

_____

_____

Reason for the revision: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Thank you!