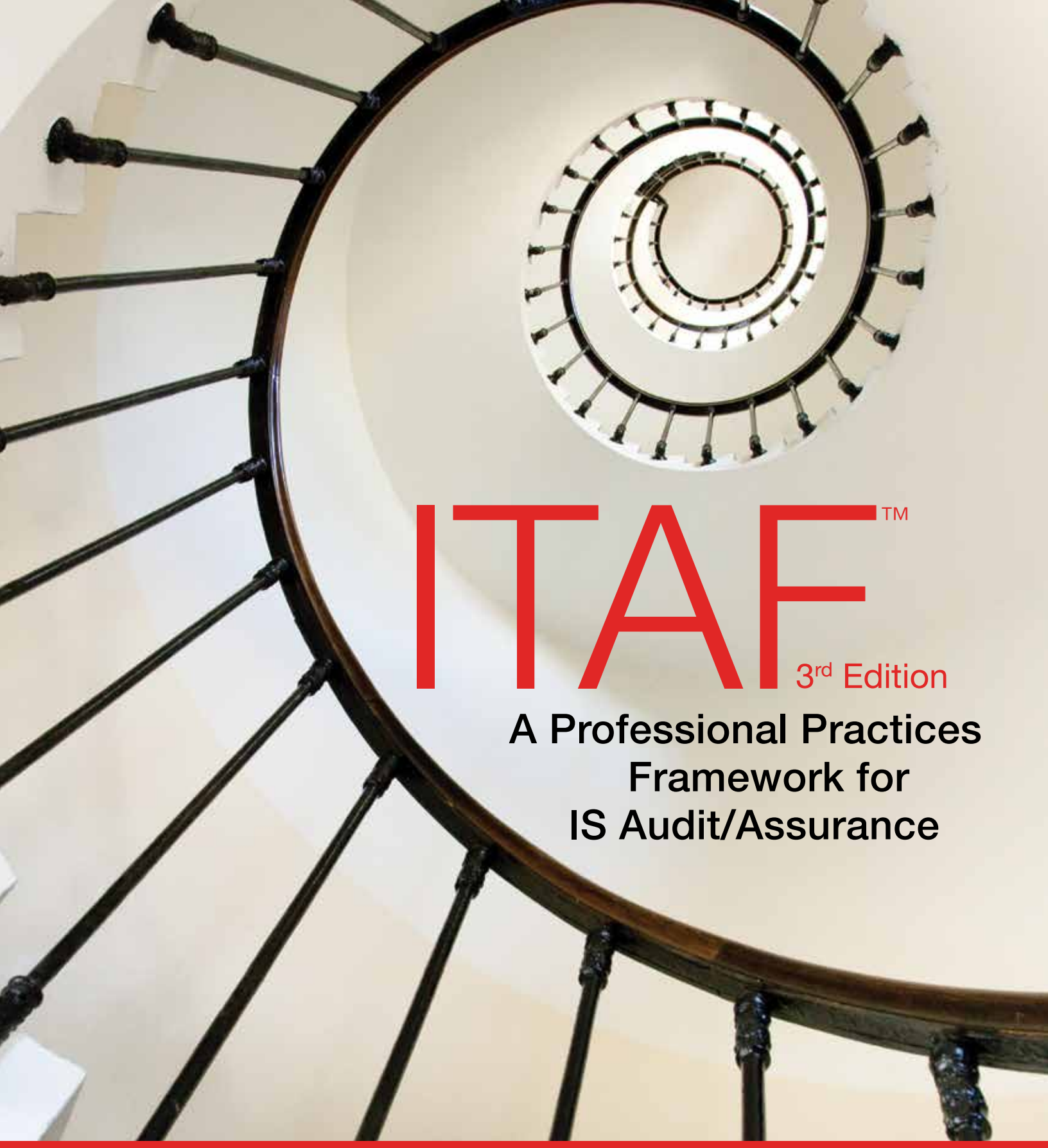

ITAF™

3rd Edition

A Professional Practices Framework for IS Audit/Assurance

ISACA®

Trust in, and value from, information systems

About ISACA®

With more than 115,000 constituents in 180 countries, ISACA® (*www.isaca.org*) helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy and governance professionals. ISACA offers the Cybersecurity Nexus™, a comprehensive set of resources for cybersecurity professionals, and COBIT®, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical 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™) credentials. The association has more than 200 chapters worldwide.

Disclaimer

ISACA has designed and created *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd 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.

ITAF 2nd Edition incorporated ISACA IS audit and assurance standards and guidance effective 1 November 2013. ITAF 3rd Edition incorporates guidelines effective 1 September 2014. As new guidance is developed and issued, it will be indexed within 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*.

The definitions apply to the most common types of engagements performed by the IS audit and assurance professional. These definitions are consistent with those provided by the American Institute of Certified Public Accountants (AICPA) and the International Auditing and Assurance Standards Board (ISAAB); however, professionals should consult the most current, original source standards relevant to the specific type of engagement(s) to be performed to ensure the most current, appropriate professional standards are followed.

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

General Guidelines

The general guidelines are:
2001 Audit Charter
2002 Organisational Independence
2003 Professional Independence
2004 Reasonable Expectation
2005 Due Professional Care
2006 Proficiency
2007 Assertions
2008 Criteria

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

2001 Audit Charter

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to assist IS audit and assurance professionals in preparing an audit charter. The audit charter defines the purpose, responsibility, authority and accountability of the IS audit and assurance function.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1001 Audit Charter
1.2.2 Standard 1002 Organisational Independence
1.2.3 Standard 1003 Professional Independence

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key IS audit and assurance engagement topics:
2.1 Mandate
2.2 Contents of audit charter

2.1 Mandate

2.1.1 Professionals should have a clear mandate to perform the audit function. This mandate is normally documented in an audit charter that should be formally approved by those charged with governance, e.g., board of directors and audit committee. Where an audit charter exists for the audit function as a whole, the IS audit and assurance mandate should be incorporated.

2001 Audit Charter *(cont.)*

2.2 Contents of Audit Charter

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

2.2.2 **Purpose** of the audit charter and audit function should contain the following sections:

- Aims/goals of the audit charter provide a functional and organisational framework in which the audit function operates.
- Mission statement and objectives of the audit function bring a structured approach to evaluate and improve the design and operational effectiveness of the risk management processes, internal control system and governance structures of information systems.
- Scope of the audit function is for either the entire enterprise or a specific organisation within the enterprise.
- Governance details the authorising body for the audit charter and audit function.

2.2.3 **Responsibility** of the audit function should contain the following sections:

- Operating principles provide a more detailed and quantitative enumeration of the different objectives of the audit function.
- Independence details the implementation of the independence requirement for the audit function and professionals, as described in Standards 1002 Organisational Independence and 1003 Professional Independence.
- Relationship with external audit details the relationship of the audit function with the external auditor:
  - Meeting with the external auditors to coordinate the work effort to minimise duplication efforts
  - Providing access to the professionals' working papers, documentation and evidence
  - Taking into account the planned work by the external auditors when drafting the audit plan for the coming period
- Auditee expectations details the services and deliverables the auditees can expect from the audit function and professionals:
  - Description of identified problems, consequences and possible resolutions relating to the area of responsibility of the auditee
  - Possibility to include management response and corrective actions taken on findings in the audit report. This includes references to related service level agreements (SLAs) for items such as delivery of reports, response to auditee complaints, quality of service, review of performance, reporting process and agreement of findings.
- Auditee requirements detail the responsibilities of the auditee, e.g., all auditees are required to make themselves available and assist the audit function and professionals in fulfilling assigned responsibilities.
- Communication with auditees details the frequency and communication channels through which the audit function will communicate with the auditees.

2.2.4 **Authority** of the audit function should contain the following sections:

- Right of access to relevant information, systems, personnel and locations by professionals when performing an audit engagement. The audit function, represented by professionals:
  - Is authorised, full, free and unrestricted access to any and all records, documentation, systems and locations when performing an audit engagement and can seek assistance from executive management in obtaining this access
  - Has the authority to seek any information from an employee, consultant or contractor when performing an audit engagement
- Limitations of authority of the audit function and professionals, if any
- Processes to be audited, which the audit function is authorised to audit, e.g., the audit function is free to determine the processes it will audit, based on the risk-based audit plan

2.2.5 **Accountability** of the audit function should contain the following sections:

- Organisational structure, including reporting lines to board and senior management, of the audit function, e.g., the audit function should have open and unrestricted access to the board and its members
- Reporting that details the format, content and recipients of the communication on the outcome of every audit engagement, e.g., a written audit report will be issued by the audit function after every audit engagement and distributed to the appropriate stakeholders, including scope, actions performed, findings, recommendations, management's response and corrective actions taken
- Performance of the audit function that details the periodic reporting process to the board on the performance of the audit function compared to the audit plan and budget, e.g., the audit function will report every quarter to the board on its purpose, responsibility and authority, as well as performance relative to the audit plan and budget

2001 Audit Charter *(cont.)*

2.2 Contents of Audit Charter (cont.)

2.2.5 *(cont.)*
- Compliance with standards that details the standards with which the audit function and professionals will adhere, e.g., the audit function and professionals will adhere and act according to all the ISACA IS Audit and Assurance Standards and Guidelines
- Quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) that establishes an understanding of auditees' needs and expectations relevant to the audit function. These needs should be evaluated against the audit charter with a view to improving the service or changing the service delivery or audit charter, as necessary. Independent external quality reviews enable the audit function to assess its compliance with applicable standards, the enterprise's risk and control framework, optimal use of resources and use of good practices. An independent external quality review of the audit function should be performed at least every five years to maintain conformance with the ISACA IS Audit and Assurance Standards.
- Staffing rules for audit engagements, e.g., establishing a minimum time period before which professionals will not be staffed on audit engagements in areas where they performed non-audit services that impair independence. The audit charter should also establish whether professionals are permitted to be involved in performing non-audit services and the broad nature, timing and extent of such services, to ensure that independence is not impaired. This could eliminate or minimise the need to obtain specific mandates for each non-audit service on a case-by-case basis.
- Continuous education commitment of the audit function toward the professionals, e.g., the audit function commits itself to provide professionals with a minimum of 40 hours of training per year
- Agreed actions regarding the audit function's and professionals' behaviour, e.g., penalties when either party fails to carry out its responsibilities

2.2.6 Other aspects that should be considered to add in the audit charter are:
- Reviewing and amending the charter, which is the responsibility of the audit function. It should periodically assess whether the purpose, responsibility, authority and accountability, as defined in the audit charter, continue to be adequate and communicate the result of the assessment to the audit committee.
- Obtaining approval of amendments to the audit charter from those charged with governance.
- Including related documents such as referencing related standards, guidelines, policies, frameworks, manuals, etc.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1001 Audit Charter	The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability. 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	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	IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.

2001 Audit Charter *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 process
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
MEA02 Monitor, evaluate and assess the system of internal controls.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and, thus, provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
- Colleagues from within the enterprise
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Audit charter	A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal IS audit and assurance activity The charter should: • Establish the internal IS audit and assurance 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 IS audit and assurance 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.

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit and assurance engagements beginning on or after 1 September 2014.

2002 Organisational Independence

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to address the independence of the IS audit and assurance function in the enterprise. Three important aspects are considered:
- The position of the IS audit and assurance function within the enterprise
- The level to which the IS audit and assurance function reports to within the enterprise
- The performance of non-audit services within the enterprise by IS audit and assurance management and IS audit and assurance professionals

1.1.2 This guideline provides guidance on assessing organisational independence and details the relationship between organisational independence and the audit charter and audit plan.

1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1001 Audit Charter
1.2.2 Standard 1002 Organisational Independence
1.2.3 Standard 1003 Professional Independence
1.2.4 Standard 1004 Reasonable Expectation
1.2.5 Standard 1006 Proficiency

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key IS audit and assurance engagement topics:
2.1 Position in the enterprise
2.2 Reporting level
2.3 Non-audit services
2.4 Assessing independence
2.5 Audit charter and audit plan

2002 Organisational Independence *(cont.)*

2.1 Position in the Enterprise

2.1.1 To enable organisational independence, the audit function needs to have a position in the enterprise that allows it to perform its responsibilities without interference. This can be achieved by:
- Establishing the audit function in the audit charter as an independent function or department, outside of the operational departments. The audit function should not be assigned any operational responsibilities or activities.
- Ensuring that the audit function reports to a level within the enterprise that allows it to achieve organisational independence. Reporting to the head of an operational department could compromise organisational independence, as described in more detail in section 2.2.

2.1.2 The audit function should avoid performing non-audit roles in IS initiatives that require assumption of management responsibilities, because such roles could impair future independence. The independence and accountability of the audit function should be addressed in the audit charter, as described in Standard 1001 Audit Charter.

2.2 Reporting Level

2.2.1 The audit function should report to a level within the enterprise that allows it to act with complete organisational independence. The independence should be defined in the audit charter and confirmed by the audit function to the board of directors and those charged with governance on a regular basis, at least annually.

2.2.2 To ensure organisational independence of the audit function, the following should be reported to those charged with governance (e.g., the board of directors) for their input and/or approval:
- The audit resource plan and budget
- The (risk-based) audit plan
- Performance follow-up performed by the audit function on the IS audit activity
- Follow-up of significant scope or resource limitations

2.2.3 To ensure organisational independence of the audit function, explicit support is needed from both the board and executive management.

2.3 Non-audit Services

2.3.1 In many enterprises, the expectation of management and IS staff is that the audit function may be involved in providing non-audit services. This involves, full-time or part-time, participation of the professionals in IS initiatives and IS project teams to provide advisory or consultative capabilities.

2.3.2 Activities that are routine and administrative or involve matters that are insignificant generally are deemed not to be management responsibilities and, therefore, would not impair independence. Non-audit services that would also not impair independence or objectivity, if adequate safeguards are implemented, include providing routine advice on information technology risk and controls.

2.3.3 The following non-audit services are considered to impair independence and objectivity, because the threats created would be so significant that no safeguards could reduce them to an acceptable level:
- Assuming management responsibilities or performing management activities
- Material involvement of professionals in the supervision or performance of designing, developing, testing, installing, configuring or operating information systems that are material or significant to the subject matter of the audit or assurance engagement
- Designing controls for information systems that are material or significant to the subject matter of current or planned future audit engagements
- Serving in a governance role where the professionals are responsible for either independently or jointly making management decisions or approving policies and standards
- Providing advice that forms the primary basis of management decisions

2.3.4 Providing non-audit services in areas that currently are, or in the future will be, the subject matter of an audit engagement also creates threats to independence that would be difficult to overcome with safeguards. In this situation, the perception may be that both the independence and objectivity of the audit function and professionals have been impaired by performing non-audit services in that specific area. The audit function and professionals should determine if adequate safeguards can be implemented to sufficiently mitigate these actual or perceived threats to independence.

2.3.5 More detailed guidance on dealing with these independence threats can be found in Standard 1003 Professional Independence and the related Guideline 2003.

2002 Organisational Independence *(cont.)*

2.4 Assessing Independence

2.4.1 Independence should be assessed regularly by the audit function and professionals. This assessment needs to occur on an annual basis for the audit function and prior to each engagement for professionals, as described in Standard 1003 Professional Independence. The assessment should consider factors such as:
- Changes in personal relationships
- Financial interests
- Prior job assignments and responsibilities

2.4.2 The audit function needs to disclose possible issues related to organisational independence and discuss them with the board of directors or those charged with governance. A resolution needs to be found and confirmed in the audit charter or audit plan.

2.5 Audit Charter and Audit Plan

2.5.1 The audit charter should detail, under the aspect 'responsibility', the implementation of organisational independence of the audit function. Next to detailing independence, the audit charter should also include possible impairments to independence.

2.5.2 Organisational independence should also be reflected in the audit plan. The audit function needs to be able to determine the scope of the plan independently, without restrictions being imposed by executive management.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1001 Audit Charter	The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability. 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	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	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	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.
1006 Proficiency	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.

2002 Organisational Independence *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM01 Ensure governance framework setting and maintenance.	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.
APO01 Manage the IT management framework.	Provide a consistent management approach to enable the enterprise governance requirements to be met, covering management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
- Colleagues within and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
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.
Objectivity	The ability to exercise judgement, express opinions and present recommendations with impartiality

5. Effective Date

5.1 Effective Date

This guideline is effective for all IS audit and assurance engagements beginning on or after 1 September 2014.

2003 Professional Independence

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. References and mapping
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to provide a framework that enables the IS audit and assurance professional to:
- Establish when independence may be, or may appear to be, impaired
- Consider potential alternative approaches to the audit process when independence is, or may appear to be, impaired
- Reduce or eliminate the impact on independence of IS audit and assurance professionals performing non-audit roles, functions and services
- Determine disclosure requirements when required independence may be, or may appear to be, impaired

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1002 Organisational Independence
1.2.2 Standard 1003 Professional Independence
1.2.3 Standard 1005 Due Professional Care

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key IS audit and assurance engagement topics:
2.1 Conceptual framework
2.2 Threats and safeguards
2.3 Managing threats
2.4 Non-audit services or roles
2.5 Non-audit services or roles that do not impair independence
2.6 Non-audit services or roles that do impair independence
2.7 Relevance of independence when providing non-audit services or roles
2.8 Governance of the admissibility of non-audit services or roles
2.9 Reporting

2003 Professional Independence *(cont.)*

2.1 Conceptual Framework

2.1.1 Many different circumstances or combinations of circumstances may be relevant in assessing threats to independence. It is impossible to define every situation that creates a threat to independence and to specify the appropriate action. Therefore, this guideline establishes a conceptual framework that requires the professional to identify, evaluate and address threats to independence. The conceptual framework approach assists in complying with the independence standards, and it accommodates many variations in circumstances that create threats to independence.

2.1.2 The conceptual framework approach should be applied by professionals to:
- Identify threats to independence.
- Evaluate the significance of the threats identified.
- Apply safeguards, when necessary, to eliminate the threats or reduce them to acceptable levels.

2.1.3 When professionals determine that appropriate safeguards are not available or cannot be applied to eliminate threats or reduce threats to an acceptable level, professionals should eliminate the circumstance or relationship creating the threats, or decline or terminate the audit or assurance engagement. If professionals cannot decline or terminate the engagement, appropriate disclosure of the impairment to independence must be made to those charged with governance and in any report resulting from the engagement.

2.1.4 Professionals should use professional judgement in applying this conceptual framework.

2.1.5 An important aspect when applying the framework is consultation. The IS audit and assurance professional should seek guidance, when considered necessary, from:
- Colleagues inside the enterprise
- Management
- Those charged with governance
- Relevant professional organisations

2.1.6 Although there is no requirement for professionals to be independent to perform non-audit services or roles, objectivity is still a professional requirement when performing them. Professionals should consider applying this conceptual framework to identify threats to objectivity, evaluate the significance of the threats and implement appropriate safeguards when performing non-audit services or roles.

2.2 Threats and Safeguards

2.2.1 Threats may be created by a broad range of relationships and circumstances. When a relationship or circumstance creates a threat, such a threat could impair, or could be perceived to impair, professional independence. A circumstance or relationship may create more than one threat to independence. Threats fall into one or more of the following categories:
- **Self-interest**—The threat that a financial or other interest will influence professional judgement or behaviour inappropriately
- **Self-review**—The threat that professionals will not appropriately evaluate the results of a previous judgement made or service performed by them or by another individual within the audit function, on which professionals will rely when forming a judgement as part of performing the current engagement
- **Advocacy**—The threat that professionals will promote an auditee's position to the point that professional objectivity is compromised
- **Familiarity**—The threat that due to a long or close relationship with the auditee, professionals will be too sympathetic to the interests of the auditee or will be too accepting of the auditee's work, views or arguments
- **Intimidation**—The threat that professionals will be deterred from acting with integrity and objectivity because of actual or perceived pressures, including attempts to exercise undue influence over professionals
- **Bias**—The threat that professionals will, as a result of political, ideological, social, psychological or other convictions, take a position that is not objective
- **Management participation**—The threat that results from professionals taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit or assurance engagement

2003 Professional Independence *(cont.)*

2.2 Threats and Safeguards (cont.)

2.2.2 Safeguards are controls designed to eliminate threats to independence or to reduce them to an acceptable level. Under the conceptual framework, professionals apply safeguards that address the specific facts and circumstances under which threats to independence exist. In some cases, multiple safeguards may be necessary to address a threat.

Examples of safeguards that can be considered by professionals in response to identified threats are:

- A governance structure at the enterprise and audit function that provides appropriate oversight and communications regarding the IS audit and assurance services to be performed
- Ensuring that professionals (and IS audit management) report to an adequate hierarchical level within the enterprise, preferably those charged with governance
- Internal procedures at the enterprise and audit function that ensure objective choices in assigning engagements, e.g., adequate educational, training and experience requirements, continuing professional development requirements
- Assigning management and staff from outside the audit function, such as borrowing staff from another function, division, external organisation, to supplement professionals
- An adequate system of incentives (rewards and penalties) that rewards professionals for critical and objective thinking and penalises bias or prejudice
- A periodic rotation in IS audit assignments of professionals reducing the degree of familiarity and self-review
- Adequate hiring practices such as background screening and vetting, which could improve the likelihood that professionals are free from bias or self-interest
- Removing an individual from an IS audit team when that individual's interests or relationships pose a threat to independence
- Appropriate documentation and reporting requirements ensuring that assessment of professional independence is documented in the work papers and consistently reported in deliverables
- Having a professional staff member or management from within the audit function who was not a member of the IS audit team carefully review the work performed
- Assigning an independent resource, from within the audit function or other sources referenced previously, to carry out a peer review or to act as an independent observer during planning, field work and reporting
- Having an external review of the reports, communications or information produced by professionals by a recognised third party, e.g., accepted authority in the field or independent specialist
- Outsourcing the IS audit and assurance engagement to an external service provider

2.3 Managing Threats

2.3.1 Facts and circumstances that create threats to independence can result from events such as the start of a new audit, assignment of new staff to an ongoing audit and acceptance of a non-audit service at an audited entity. Many other events can result in threats to independence. Whenever relevant new information about a threat to independence comes to the attention of professionals during an audit or assurance engagement, they should re-evaluate the significance of the threat in accordance with the conceptual framework.

2.3.2 Professionals should evaluate threats:

- To independence using the conceptual framework when the facts and circumstances under which professionals perform their work may create new threats or increase the significance of existing threats to independence
- Both individually and in the aggregate because threats can have a cumulative effect on professional independence
- Both qualitatively and quantitatively when determining the significance of a threat

2.3.3 The audit function and professionals should determine whether identified threats to independence are at an acceptable level or have been eliminated or reduced to an acceptable level. A threat to independence is not acceptable if it could either:

- Impact a professional's ability to perform an audit or assurance engagement without being affected by influences that compromise professional judgement
- Expose professionals, audit function or audit organisation to circumstances that would cause a reasonable and informed third party to conclude that the integrity, objectivity or professional scepticism of the audit organisation, or a member of the IS audit and assurance team, had been compromised

2003 Professional Independence *(cont.)*

2.3 Managing Threats (cont.)

2.3.4 When the audit function and professionals identify threats to independence and, based on an evaluation of those threats, determine that the threats are not at an acceptable level, they should:
- Determine whether appropriate safeguards are available and can be applied to eliminate the threats or reduce them to acceptable levels.
- Exercise professional judgement in making that determination, and should take into account whether both independence of mind and independence in appearance are maintained.
- Seek guidance from appropriate parties, as described in 2.1.5, to identify and apply appropriate safeguards.

2.3.5 Documentation provides evidence of professionals' judgements in forming conclusions regarding compliance with independence requirements.

2.3.6 Professionals should document conclusions regarding compliance with independence requirements and the substance of any relevant discussions with audit management and, if necessary, those charged with governance, that support those conclusions, including the:
- The steps that were taken to analyse the nature of independence
- The actual nature of the independence issue
- List and description of threats
- The final conclusion reached
- Safeguards in place to eliminate or reduce the threats to an acceptable level

2.4 Non-audit Services or Roles

2.4.1 In many enterprises, the expectation of management, IS staff and internal audit is that professionals may be involved in providing non-audit services or roles such as:
- Defining IS strategies relating to areas such as technology, applications and resources
- Evaluating, selecting and implementing technologies
- Evaluating, selecting, customising and implementing third-party IS applications and solutions
- Designing, developing and implementing custom-built IS applications and solutions
- Establishing good practices, policies and procedures relating to various IT functions
- Designing, developing, testing and implementing IT security and IT controls
- Managing IT projects

2.4.2 Providing non-audit services or roles, in general, involves full-time or part-time participation in IT initiatives and IT project teams to provide advisory or consultative capabilities. IS audit and assurance professionals may fulfil a non-audit function through activities such as:
- The full-time temporary assignment or loan of IS audit and assurance staff to an IT project team
- The part-time assignment of an IS audit and assurance staff member as a member of the various IT 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 advisor or reviewer of IT projects or IT controls on an ad hoc basis

2.4.3 Providing non-audit services or roles may create threats to professional independence in attitude or appearance that can be particularly difficult to overcome with safeguards if the area in which the non-audit services or roles were performed currently is, or in the future becomes, the subject matter of an audit or assurance engagement. In this situation, the perception may be that both the independence and the objectivity of professionals have been impaired by performance of the non-audit services or roles.

2.4.4 Professionals providing non-audit services or roles should evaluate, using the conceptual framework, whether the non-audit services or roles generate an impairment of independence either in attitude or in appearance for current or future audit or assurance engagements. This applies to engagements where the area in which the non-audit services or role is performed is significant or materiality to the subject matter or stakeholders of those engagements. Professionals should seek guidance from IS audit and assurance colleagues and management when necessary, and also, if necessary, from those charged with governance, to determine if adequate safeguards can be implemented to adequately mitigate any actual or perceived threats to independence.

2003 Professional Independence *(cont.)*

2.4 Non-audit Services or Roles (cont.)

2.4.5 Prior to commencing non-audit services or roles, professionals should establish and document their understanding with IS audit management and/or those charged with governance, as appropriate, regarding:
- The objectives of the non-audit services or roles
- The nature of the non-audit services or roles to be performed
- The audited entity's acceptance of its responsibilities related to the non-audit services or roles
- Professional responsibilities related to the non-audit services or roles
- Any limitations of the non-audit services or roles
- Any limitations to the scope of future audit services professionals can provide

2.4.6 In the case of an IS audit or assurance engagement where there is potential for impaired independence in attitude or appearance due to non-audit services or roles performed, IS audit and assurance management should implement safeguards such as:
- Monitoring the conduct of the audit closely
- Evaluating any significant indications of impairment of independence in attitude or appearance arising out of non-audit services or roles performed and initiating necessary safeguards
- Informing those charged with governance of the potential impairment of independence in attitude or appearance and the safeguards implemented

---

2.5 Non-audit Services or Roles That Do Not Impair Independence

2.5.1 Activities that are routine and administrative or involve matters that are insignificant generally are deemed not to be a management responsibility and therefore would not impair independence. Further, providing advice and recommendations to assist management in discharging its responsibilities is not regarded as assuming a management responsibility.

2.5.2 Non-audit services or roles that would also not impair independence or objectivity if adequate safeguards are implemented include providing routine advice on IT risk and controls.

2.5.3 To avoid the risk of assuming a management responsibility when providing non-audit services or roles in an area that is or could become the subject of an audit or assurance engagement, professionals should only provide the non-audit services or roles if satisfied that management performs or will perform the following functions in connection with the non-audit services or roles:
- Assume all management responsibilities
- Oversee the services by designating an individual, preferably within senior management, who possesses suitable skill, knowledge or experience
- Evaluate the adequacy and results of the services performed
- Accept responsibility for the results of the services

Professionals should document consideration of management's ability to effectively oversee the non-audit services or roles to be performed.

2003 Professional Independence *(cont.)*

2.6 Non-audit Services or Roles That Do Impair Independence

2.6.1 If professionals were to assume management responsibilities or perform management activities, the threats to independence could become so significant that no safeguards could reduce them to an acceptable level. Whether an activity is a management responsibility depends on the circumstances and requires the exercise of professional judgement. Examples of activities that would generally be considered a management responsibility include:

- Setting policies and strategic direction
- Directing and taking responsibility for the actions of the entity's employees
- Authorising transactions
- Deciding which recommendations of the audit function, internal audit function, organisation, firm or other third parties to implement
- Taking responsibility for designing, implementing or maintaining internal control
- Accepting responsibility for the management of an IT project or initiative

2.6.2 In addition to assuming management responsibilities, the following non-audit services or roles are considered to impair independence and objectivity:

- Material involvement of professionals in the supervision or performance of designing, developing, testing, installing, configuring or operating information systems that are material or significant to the subject matter of the audit or assurance engagement
- Designing controls for information systems that are material or significant to the subject matter of the audit or assurance engagement
- Serving in a governance role where professionals are responsible for either independently or jointly making management decisions or approving policies and standards
- Providing advice that forms the primary basis of management decisions or performing management functions

2.7 Relevance of Independence When Providing Non-audit Services or Roles

2.7.1 Unless prohibited by other external standards or by legislation, there is no requirement for professionals either to be, or to be seen to be, independent when carrying out tasks relating to performing non-audit services or roles; objectivity is still a professional requirement. Accordingly, professionals should carry out tasks relating to non-audit services or roles in an objective and professional manner.

2.7.2 Despite there being no requirement for professionals to be independent while performing non-audit services or roles, professionals should consider whether independence could be impaired if they are assigned to perform an audit or assurance engagement in which the area where non-audit services or roles are or were provided is material to the subject matter of the engagement. Where such a potential impairment is foreseeable (e.g., where an independent audit will be required later and there is only one professional with the requisite skills to perform both the non-audit services or roles and the subsequent audit), the professional should seek guidance from audit management and, if necessary, those charged with governance, prior to accepting or performing the non-audit services or roles.

2.7.3 Determining whether professionals should perform non-audit services or roles, when a current or subsequent audit or assurance engagement of the area where the non-audit services or roles is planned or likely performed by the same professional, should be the decision of IS audit management with the concurrence of those charged with governance. IS audit management should apply the conceptual framework when making a decision, and the following factors may also influence the decision:

- Professionals should not be placed into a situation to audit their own work or provide non-audit services or roles to areas that are known or likely to be significant or material to the subject matter of IS audit or assurance engagements in which they are or will be involved
- Whether there are available resources to perform both the non-audit and independent audit and assurance function separately
- The IS management's and those charged with governance perception of the value or importance of the non-audit services or roles relative to the audit and assurance engagement
- Level of risk to the audit function associated with the non-audit services or roles
- Effect of the decision on the requirements of external auditors or regulators, if any
- The provisions of the IS audit charter

2003 Professional Independence *(cont.)*

2.8 Admissibility of Non-audit Services or Roles

2.8.1 The IS audit charter should establish whether professionals are permitted to be involved in performing non-audit services or roles and the broad nature, timing and extent of such services or roles, to ensure that independence is not impaired with respect to the systems they may audit. This could eliminate or minimise the need to obtain specific mandates for each non-audit service or role on a case-by-case basis.

2.8.2 Professionals should provide reasonable assurance that the terms of reference (TOR) of specific non-audit services or roles are in conformity with the audit charter. Where there are any deviations, the same should be expressly spelled out in the TOR and approved by IS audit and assurance management and/or those charged with governance.

2.8.3 Where the audit charter does not specify the non-audit services or roles or where there is no audit charter, professionals should report the nature of their involvement in non-audit services or roles to IS audit and assurance management and those charged with governance. The timing and extent of professionals' involvement in non-audit services or roles should be subject to individual TOR signed by management of the function where the services or roles will be performed and approved by those charged with governance.

2.9 Reporting

2.9.1 Where the independence of professionals, with reference to an IS audit or assurance engagement, could be, could appear to be, or is impaired, and those charged with governance have made the decision to continue the engagement, the IS audit and assurance engagement report should include sufficient information to allow the users of the report to understand the nature of the potential impairment. Information that professionals should consider disclosing in an IS audit and assurance engagement report includes:

- Names and seniority of professionals involved in the IS audit or assurance engagement that may have, or may appear to have, an impairment to independence
- Analysis and description of the threats to independence
- Safeguards implemented to eliminate or mitigate different threats to independence and objectivity during the course of the engagement work and the reporting process
- The fact that the potential impairment of independence has been disclosed to those charged with governance and their approval to perform or continue the assurance engagement and/or the non-audit services or roles

---

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

For the standards only the relevant clauses are listed.

2003 Professional Independence *(cont.)*

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed

Standard Title	Relevant Standard Statements
1001 Audit Charter	The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability. 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	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	IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.
1005 Due Professional Care	IS audit and assurance professionals shall exercise due care, including observance of applicable professional audit standards, in planning, performing and reporting on the results of engagements.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
- Colleagues within and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the enterprise, e.g., audit committee

2003 Professional Independence *(cont.)*

4. Terminology

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 an IS audit team's, or a member of the IS 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.
Integrity	The guarding against improper information modification or destruction, which includes ensuring information non-repudiation and authenticity
Materiality	An audit concept regarding the importance of an item of information with regard to its impact or effect on the subject matter being audited. An expression of the relative significance or importance of a particular matter in the context of the engagement or the enterprise as a whole.
Objectivity	The ability to exercise judgement, express opinions and present recommendations with impartiality
Professional judgement	The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement
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

5. Effective Date

5.1 Effective Date This guideline is effective for all IS audit and assurance engagements beginning on or after 1 September 2014.

2004 Reasonable Expectation

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to assist the IS audit and assurance professionals in implementing the principle of reasonable expectation in the execution of audit engagements. The main features over which the professionals should have reasonable expectation are that:
- The audit engagement can be completed in accordance with these standards, other applicable standards or regulations, and result in a professional opinion or conclusion.
- The scope of the audit engagement permits an opinion or conclusion to be expressed on the subject matter.
- Management will provide them with appropriate, relevant and timely information required to perform the audit engagement.

1.1.2 This guideline further assists the IS audit and assurance professionals in addressing scope limitations and provides guidance on accepting a change in terms.

1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1001 Audit Charter
1.2.2 Standard 1004 Reasonable Expectation

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Standards and regulations
2.2 Scope
2.3 Scope limitations
2.4 Information
2.5 Acceptance of a change in engagement terms

2004 Reasonable Expectation *(cont.)*

2.1 Standards and Regulations

2.1.1 The audit charter will determine the standards the audit function and professionals will adhere to, as described in Standard 1001 Audit Charter.

2.1.2 Professionals should gather and assess all applicable standards listed in the audit charter and regulations before the audit engagement and revisit them throughout the engagement to determine if they have reasonable expectation that they can complete the audit engagement in accordance with these standards and regulations, and that the audit engagement will result in a professional opinion or conclusion.

2.1.3 Should professionals determine that the audit engagement cannot be completed in accordance with one or more of the applicable standards and regulations, and thus expressing a professional opinion or conclusion will not be possible, they should:
- Inform IS audit and assurance management and those charged with governance of the identified compliance issues with the standards and regulations
- Propose either a change in engagement terms or that the proposed engagement not be accepted

2.2 Scope

2.2.1 Before undertaking the audit engagement, the professionals should review the scope of the audit engagement. They should determine that the scope of the audit is clearly documented and permits a professional opinion or conclusion to be drawn on the subject matter.

2.2.2 The scope of the audit engagement should be clearly documented, with no room for interpretation as to which areas (e.g., processes, activities, systems) are in scope of the engagement. A scope that is described too vaguely will not allow professionals to form a professional opinion or conclusion, because there is no certainty that all areas in scope are assessed.

2.2.3 Should professionals determine that the scope of the audit engagement does not enable them to express a professional opinion or conclusion, they should:
- Inform IS audit and assurance management and those charged with governance of the identified issues with the scope.
- Propose a change in engagement terms or not accept the proposed audit engagement.

2.3 Scope Limitations

2.**3.1** Specific scope limitations may occur before or during the audit engagement. These scope limitations can be influenced by different factors, such as:
- Appropriate, relevant and timely information required to complete the audit engagement is unavailable.
- (Key) auditees are unavailable.
- The time frame included is insufficient to complete the entire scope of the audit engagement.
- Management tries to limit the scope of the audit engagement to selected areas.
- The scope of the audit engagement is either too small or too large to come to a conclusion on the subject matter.
- The level of decentralisation makes it difficult to come to a conclusion on the totality of the subject matter.
- Availability of sufficient number of appropriately skilled professionals to perform the audit engagement with its current scope.
- The reporting structure of the audit function, e.g., if the audit function does not report to the appropriate level within the enterprise, it may be directed not to assess certain elements in scope

2.3.2 The professionals should consider whether these scope limitations still allow for reasonable expectation that the audit engagement will result in a professional opinion or conclusion. Should they determine that this condition will not be fulfilled, they should not accept the engagement.

2.3.3 Should professionals conclude that they still have reasonable expectation that, despite the scope limitations, the engagement will result in a professional opinion or conclusion, professionals should accept or continue the audit engagement. The scope limitations should be explicitly described in the IS audit and assurance engagement report.

2004 Reasonable Expectation *(cont.)*

2.4 Information

2.4.1 The audit charter will determine the right of access to information, systems, personnel and locations relevant to the performance of the audit engagement, as described in Standard 1001 Audit Charter.

2.4.2 Before undertaking the audit engagement, professionals need to identify and address any restrictions being placed upon their right to access appropriate, relevant and timely information for the audit engagement. They should have a reasonable expectation that their right to access for this audit engagement is in accordance with the stipulations in the audit charter, or that potential deviations from these stipulations do not preclude the professionals from reaching a professional opinion or conclusion on the subject matter.

2.4.3 Performing an audit or assurance engagement could involve assessing activities performed by senior and executive management. The possibility of such an event occurring should be assessed before the execution of the audit engagement as well as whether professionals will be challenged in their need to access these individuals or related information. Mitigating actions might be needed before the execution of the audit engagement such as, but not limited to:

- Ensuring the audit charter provides appropriate authority to the audit function and professionals
- Obtaining the explicit, written support from those charged with governance, e.g., board of directors and audit committee
- Attendance by a member of the board or executive management when requiring access to executive or senior management

2.4.4 Should professionals conclude that their right of access to information does not enable them to express a professional opinion or conclusion, they should:

- Inform IS audit and assurance management and those charged with governance of the identified issues with their right to access appropriate, relevant and timely information.
- Propose a change in engagement terms or not accept the proposed audit engagement.

2.5 Acceptance of a Change in Engagement Terms

2.5.1 Professionals should not accept a change in terms of the audit engagement when there is no justification for doing so, based on their professional judgement.

2.5.2 If professionals, prior to the end of the audit engagement, are requested to accept a change in terms that lowers the level of assurance, they should determine whether there is justification for doing so, based on their professional judgement.

2.5.3 If the terms of an audit engagement are changed, they should be recorded and formally approved by both professionals and IS audit and assurance management. After completion of the audit engagement, the IS audit and assurance engagement report should mention this change in terms explicitly.

2.5.4 If professionals do not accept a change in terms of the audit engagement and management does not permit them to continue the original audit engagement, in consultation with audit and assurance management they should:

- Withdraw from the audit engagement.
- Determine, according to their professional judgement, the need to report the circumstances to those charged with governance, the board of directors or even regulators.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:

3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

2004 Reasonable Expectation *(cont.)*

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA Standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1001 Audit Charter	The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability. The IS audit and assurance function shall have the audit charter agreed upon and approved at an appropriate level within the enterprise.
1004 Reasonable Expectation	IS audit and assurance professionals shall have reasonable expectation that the engagement can be completed in accordance with 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. 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. 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.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process ID and Title	Process Purpose
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
- Colleagues from within and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

2004 Reasonable Expectation *(cont.)*

4. Terminology

Term	Definition
(None)	

5. Effective Date

5.1 Effective Date This guideline is effective for all IS audit and assurance engagements beginning on or after 1 September 2014.

2005 Due Professional Care

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to clarify the term 'due professional care' as it applies to performing an audit engagement with integrity and care in compliance with the ISACA Code of Professional Ethics.

1.1.2 This guideline explains how IS audit and assurance professionals should apply due professional care in planning, performing and reporting on an audit engagement.

1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1002 Organisational Independence
1.2.2 Standard 1003 Professional Independence
1.2.3 Standard 1005 Due Professional Care
1.2.4 Standard 1006 Proficiency
1.2.5 Standard 1205 Evidence

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Professional scepticism and competency
2.2 Application
2.3 Life cycle of the engagement
2.4 Communication
2.5 Managing information

2005 Due Professional Care *(cont.)*

2.1 Professional Scepticism and Competency

2.1.1 Due professional care applies to the exercise of professional judgement in the conduct of work performed. Due professional care implies that professionals should approach matters requiring professional judgement with professional scepticism, diligence, integrity and care. They should maintain this attitude throughout the whole engagement.

2.1.2 Professionals should maintain competence, independence and an objective state of mind in all matters related to the conduct of the audit engagement. They should be honest, impartial and unbiased in addressing issues and reaching conclusions.

2.1.3 Exercising due professional care should make professionals consider the possible existence of inefficiencies, misuses, errors and exclusions, incompetence, conflicts of interest, or fraud. It should also make professionals attentive for specific conditions or activities where these issues can occur.

2.1.4 By keeping informed of and complying with developments in professional standards, professionals demonstrate sufficient understanding and professional competence to achieve the IS audit and assurance objectives. Detailed guidance can be found in Standard 1006 Proficiency.

2.1.5 Professionals should conduct the audit engagement with diligence while adhering to professional standards and statutory and regulatory requirements.

2.2 Application

2.2.1 Due professional care should extend to every aspect of the audit, including, but not restricted to, evaluating audit risk, accepting audit assignments, establishing audit scope, formulating audit objectives, planning the audit, conducting the audit, allocating resources to the audit, selecting audit tests, evaluating test results, documenting the audit, arriving at audit conclusions, reporting and delivering audit results. In doing this, professionals should determine or evaluate the:

- Type, level, skill and competence of resources required to meet the IS audit and assurance objectives
- Significance of identified risk and the potential effect of such risk on the subject of the audit
- Sufficiency, validity and relevance of audit evidence gathered
- Competence, integrity and conclusions of others upon whose work professionals place reliance

2.2.2 Due professional care also requires professionals to conduct all engagements with the concept of reasonable assurance in mind.

2.2.3 Professionals 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.

2.3 Life Cycle of the Engagement

2.3.1 Professionals should plan the audit engagement completely and in a timely manner by exercising due professional care to ensure the availability of the appropriate resources and a timely completion of the audit engagement. Professionals assigned to the project should collectively possess the needed skills, knowledge and relevant competencies to perform the audit engagement.

2.3.2 Professionals should conduct the audit engagement by applying due professional care, i.e., by following the appropriate professional standards to ensure a quality and complete audit conclusion or opinion.

2.4 Communication

2.4.1 The defined roles and responsibilities should be communicated to the team members before the start of the project to ensure the team's adherence to the appropriate professional standards during the audit engagement.

2.4.2 During the audit engagement professionals should appropriately communicate with auditees and relevant stakeholders to ensure their cooperation.

2.4.3 Professionals should address their findings to auditees of the audit engagement.

2.4.4 Professionals should document and communicate concerns regarding the application of professional standards to appropriate parties to resolve concerns.

2.4.5 Professionals should exercise due professional care while informing appropriate parties of the results of work performed.

2005 Due Professional Care *(cont.)*

2.5 Obtaining and Managing Information

2.5.1 The professionals should have reasonable expectation that management understands its obligations and responsibilities in providing appropriate, relevant and timely information required for the performance of the audit engagement.

2.5.2 Professionals should take reasonable measures to maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information must not be used for personal benefit or released to inappropriate parties.

2.5.3 Information should be retained and properly disposed of in accordance with organisational policies and relevant laws, rules and regulations.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA Standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1002 Organisational Independence	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	IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.
1005 Due Professional Care	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	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. IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate knowledge of the subject matter. IS audit and assurance professionals shall maintain professional competence through appropriate continuing professional education and training.
1205 Audit Evidence	IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

2005 Due Professional Care *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes*.

COBIT 5 Process	Process Purpose
EDM01 Ensure governance framework setting and maintenance.	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.
APO07 Manage human resources.	Optimise human resources capabilities to meet enterprise objectives.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance, when considered necessary. This could be from IS audit and assurance:
- Colleagues from within the organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Professional competence	Proven level of ability, together with professional experience, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards
Professional judgement	The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement
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

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit and assurance engagements beginning on or after 1 September 2014.

2006 Proficiency

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 This guideline provides guidance to assist the IS audit and assurance professionals to acquire the necessary skills and knowledge and maintain the professional competences while carrying out audit engagements.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1005 Due Professional Care
1.2.2 Standard 1006 Proficiency
1.2.3 Standard 1201 Engagement Planning
1.2.4 Standard 1203 Performance and Supervision

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Professional competence
2.2 Evaluation
2.3 Reaching the desired level of competence

2.1 Professional Competence

2.1.1 Professional competence implies possessing skills, knowledge and expertise, through an adequate level of education and experience, to have the ability to appropriately perform an audit engagement.

2.1.2 IS audit and assurance management should communicate the desired and/or expected level of professional competence, based on appropriate benchmarks, for the different roles in audit engagements and ensure such benchmarks are periodically reviewed and updated. IS audit and assurance management should document the professional competence required for various job levels, for example by formulating a skills matrix that indicates the professional competence required for the various job levels.

2.1.3 IS audit and assurance management should provide reasonable assurance of the availability of competent resources required to carry out the audit engagements defined in the IS audit plan, and the availability of such competent resources should be confirmed and ensured prior to commencement of the audit engagement.

2.1.4 IS audit and assurance management is responsible for ensuring the team members are competent to perform the audit engagement. Identification of core professional competencies of team members will assist in efficient utilisation of available resources.

2006 Proficiency *(cont.)*

2.1 Professional Competence (cont)

2.1.5 Professionals should provide reasonable assurance that they possess the required level of professional competence. They should be responsible for acquiring the required professional and technical skills and knowledge to carry out any assignment they agree to perform.

2.1.6 The required skills and knowledge vary with the professionals' position and the role with respect to the audit engagement. Requirement for management skills and knowledge should be commensurate with the level of responsibility.

2.1.7 Skills and knowledge include proficiency in the identification and management of risk and controls, as well as audit tools and techniques. Professionals should possess analytical and technical knowledge together with interviewing, interpersonal and presentation skills.

2.1.8 Professionals should possess the knowledge to identify, determine the impact of, and communicate possible conditions or deviations that are material to the audit engagement.

2.1.9 Professionals should possess the ability to recognise possible fraud indicators.

2.1.10 Professionals should have a general knowledge of business fundamentals, e.g., economics, finance, accounting, information technology, risk, tax and law to prevent them from overlooking potential issues or shortcomings.

2.1.11 It is appropriate for professionals to share their experiences, adopted good practices, lessons learned and knowledge gained amongst team members to improve the professional competencies of the resources. The professional competencies of team members are also improved through team building sessions, workshops, conferences, seminars, lectures and other modes of interaction.

2.1.12 To ensure the availability of the appropriate skills, alternative means of acquiring these skills should be assessed. This includes subcontracting specific resources, outsourcing a portion of the IS audit and assurance tasks and/or delaying the audit engagement until the needed skills are available.

2.1.13 External knowledge can be obtained by outsourcing part of the engagement. Collaboration between outsourced resources and internal professionals ensures that knowledge and skills also are developed and maintained internally.

2.1.14 Where any part of the audit engagement is outsourced or expert assistance is obtained, reasonable assurance must be provided that the outsourced agency or the external expert possesses the requisite professional competence.

2.1.15 Where expert assistance is obtained on a continual basis, professional competence of such external experts should be periodically measured, monitored and reviewed against professional standards or benchmarks.

2.2 Evaluation

2.2.1 Professionals should monitor their skills and knowledge continually to maintain the appropriate level of professional competence. IS audit and assurance management should periodically evaluate professional competence.

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

2.2.3 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.

2.2.4 In the case of a team of professionals, evaluation should be carried out internally amongst teams or individuals on a cross-functional basis.

2.2.5 In the case of single (sole) independent professionals, 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.

2.2.6 Evaluation of the performance of professionals should be performed by an appropriate level of management.

2.2.7 Gaps noted during evaluation should be addressed appropriately.

2006 Proficiency *(cont.)*

2.3 Reaching the Desired Level of Competence

2.3.1 Gaps noted based upon variance in the actual level of professional competence to the expected level of professional competence should be recorded and analysed. Where a significant deficiency exists in any resource, such resource should not be used in conducting an audit engagement.

2.3.2 It is important to ascertain the cause for the gap and to take appropriate corrective action measures, such as training and continuing professional education (CPE), as soon as possible.

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

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

2.3.5 Documentation of the required skills, such as a skills matrix, as formulated by IS audit and assurance management (2.1.2), will aid in identifying gaps and training needs. The matrix can be cross-referenced to the available resources and their skills and knowledge.

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

2.3.7 CPE is the methodology adopted to maintain professional competence and update skills and knowledge. Professionals should adhere to the requirements of the CPE policies established by the respective professional bodies with which they are associated.

2.3.8 CPE programmes should aid in the enhancement of skills and knowledge and relate to professional and technical requirements of IS assurance, security and governance. Professional bodies ordinarily prescribe programmes eligible for CPE recognition. Professionals should adhere to such norms prescribed by their respective professional bodies.

2.3.9 Professional bodies ordinarily prescribe the methodology of attainment of CPE credits and the minimum credits that should be obtained periodically by their constituents. Professionals must adhere to such norms prescribed by their respective professional bodies. Where professionals are associated with more than one professional body for the purpose of attainment of minimum credits, they may use their professional 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.

2.3.10 ISACA has a comprehensive policy on CPE, applicable to its members and holders of the CISA designation. Professionals with the CISA designation must comply with ISACA's CPE policy. Details of the policy are available at *www.isaca.org/CISAcpepolicy.*

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

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:

3.1 Linkage to standards

3.2 Linkage to COBIT 5 processes

3.3 Other guidance

2006 Proficiency *(cont.)*

3.1 Linkage to Standards

The table provides an overview of:

- The most relevant ISACA Standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1005 Due Professional Care	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	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. IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate knowledge of the subject matter. IS audit and assurance professionals shall maintain professional competence through appropriate continuing professional education and training.
1201 Engagement Planning	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 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
1203 Performance and Supervision	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. 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.

2006 Proficiency *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM04 Ensure resource optimisation.	Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change.
APO07 Manage human resources.	Optimise human resources capabilities to meet enterprise objectives.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
- Colleagues from within the organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Materiality	An audit concept regarding the importance of an item of information with regard to its impact or effect on subject matter being audited. An expression of the relative significance or importance of a particular matter in the context of the engagement or the enterprise as a whole.
Professional competence	A proven level of ability, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards
Professional judgement	The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement
Proficiency	Possessing skill and experience

5. Effective Date

5.1 Effective Date

This guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2007 Assertions

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to detail the different assertions, guide IS audit and assurance professionals in assuring that the criteria, against which the subject matter is to be assessed, supports the assertions, and provide guidance on formulating a conclusion and drafting a report on the assertions.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1007 Assertions
1.2.2 Standard 1008 Criteria
1.2.3 Standard 1204 Materiality
1.2.4 Standard 1206 Using the Work of Other Experts
1.2.5 Standard 1401 Reporting

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Assertions
2.2 Subject matter and criteria
2.3 Assertions developed by third parties
2.4 Conclusion and report

2007 Assertions *(cont.)*

2.1 Assertions

2.1.1 Assertions are any declaration or set of declarations about whether the subject matter is based on or in conformity with the criteria selected. Professionals should consider these assertions throughout the execution of an audit engagement, obtain assurance on their achievement and express this in the audit report.

2.1.2 Common assertions that may be considered include:
- **Confidentiality**—Preserving authorised restrictions on access and disclosure, including means for protecting privacy and proprietary information
- **Completeness**—All activities, information and other data that should have been recorded are recorded, e.g., all IT system changes promoted to production are recorded in the change management tracking application
- **Accuracy**—Amounts, dates and other data related to recorded activities have been recorded appropriately, e.g., data related to the promotion of IT system changes into production are accurately displayed in the change records of the change management tracking application
- **Integrity**—Information, evidence and other data received come from trustworthy and reliable sources, e.g., the change records requested by professionals are received from the compliance manager, a trustworthy and reliable source within the enterprise
- **Availability**—Information, evidence and other data required for the audit engagement exist and are accessible, e.g., the requested change records exist and are readily accessible in the change management tracking application
- **Compliance**—Information, evidence and other data has been recorded according to the enterprise, regulatory or other applicable stipulations, e.g., required fields, according to the applicable stipulations, are present on the change records of the change management tracking application

2.1.3 Management is responsible for defining and approving subject matter and related assertions. Professionals should ensure that any assertions developed by management are what a knowledgeable reader or user would expect compared to other standards of authoritative pronouncements.

2.1.4 A precondition for professionals to accept the audit engagement should be the confirmation from management that it fully understands its responsibility to provide all required information regarding the subject matter and the assertions to professionals. If professionals believe that management will not be able to fulfil this responsibility, they should:
- Inform IS audit and assurance management and those charged with governance of the identified issue
- Not accept the proposed audit engagement

2.1.5 Professionals should review the selected assertions for the audit engagement and ensure that they are:
- **Sufficient**—Enough to meet the purpose of the audit engagement, which is expressing an opinion or conclusion on the subject matter in scope
- **Valid**—Able to be tested, given the subject matter in scope
- **Relevant**—Have a direct connection to the subject matter in scope and contribute to meeting the purpose of the audit engagement

2.2 Subject Matter and Criteria

2.2.1 The subject matter of an audit engagement is determined by management and those charged with governance. Usually, the IS audit engagement subject matter will not be as accurately defined as it is with financial audit engagements. For example, the subject matter of IS audit and assurance engagements can vary from one system and its interfaces, to a process (covering multiple systems and interfaces), or even all IS-related operations of a certain department.

2.2.2 Professionals should assess the subject matter of the audit engagement against predetermined criteria to express an opinion or conclusion on the subject matter. Professionals should evaluate these criteria to ensure that they support the relevant assertions.

2.2.3 One criterion can link to multiple assertions. On the other hand, one assertion can also be supported by multiple criteria that all provide a part of the assurance in attaining the assertion.

2.2.4 Should professionals conclude that the criteria do not fully support all of the relevant assertions, they should make suggestions for modification of the existing criteria or for adding additional criteria. IS audit and assurance management review and approve or reject the new or modified criteria.

2.2.5 Next to assessing that the criteria fully support the relevant assertions, professionals should also assess that the criteria can be subject to objective and measurable analysis, as detailed in Standard 1008 Criteria.

2007 Assertions *(cont.)*

2.3 Assertions Developed by Third Parties

2.3.1 Enterprises outsourcing operations to third parties will receive reports about the control environment of the outsourced operations. Management reviews each report to determine whether:

- The report is issued by a relevant independent professional body
- The audit opinion is qualified or unqualified
- The scope of the control objectives adequately covers the controls required by the enterprise
- The period being audited is in line with the enterprise expectation
- Specific control deficiencies (that did not lead to an overall qualification of the report) are relevant to the enterprise
- The assertions being used are in line with the required assertions

IS audit and assurance management should document the analysis made and conclusions reached. Professionals should ensure that the assertions are verified and formally approved by management, as part of an audit engagement that has the outsourced operations in scope. Standard 1206 Using the Work of Other Experts provides further guidance on this topic.

2.4 Conclusion and Report

2.4.1 After assessing the subject matter of the audit engagement against the criteria, professionals should form a conclusion on each assertion, based on the aggregate of the findings against related criteria, along with professional judgement.

2.4.2 After forming a conclusion, professionals should issue an indirect or direct report on the subject matter:

- **Indirect report**—On the assertions about the subject matter. For example, on the assertion 'completeness,' for a component of the subject matter: 'Based on our operating effectiveness testing, in our opinion the IT system changes promoted to production, in all material respects according to the selected criteria, have been completely recorded in the change management tracking application.'
- **Direct report**—On the subject matter itself. For example, on the entire subject matter: 'Based on our testing, in our opinion the IT system changes are following, in all material respect according to the selected criteria, the required change management procedure.'

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

2007 Assertions *(cont.)*

3.1 Linkage to Standards

The table provides an overview of:

- The most relevant ISACA Standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1007 Assertions	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	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.
1204 Materiality	IS audit and assurance professionals shall disclose the following in the audit report: • Absence of controls or ineffective controls • Significance of the control deficiency • Likelihood of these weaknesses resulting in a significant deficiency or material weakness
1206 Using the Work of Other Experts	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.
1401 Reporting	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

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:

- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM01 Ensure governance framework setting and maintenance.	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for the board members are met.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

2007 Assertions *(cont.)*

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:

- Colleagues from within the organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

4. Terminology

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.
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.
Professional judgement	The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement
Subject matter	The specific information subject to an IS auditor's report and related procedures, which can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations (area of activity)

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2008 Criteria

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to assist IS audit and assurance professionals in selecting criteria, against which the subject matter will be assessed, that are suitable, acceptable and come from a relevant source.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1007 Assertions

1.2.2 Standard 1008 Criteria

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Selection and use of criteria
2.2 Suitability
2.3 Acceptability
2.4 Source
2.5 Change in criteria during the audit engagement

2008 Criteria *(cont.)*

2.1 Selection and Use of Criteria

2.1.1 Professionals shall select criteria, against which the subject matter will be assessed. When selecting the criteria, professionals shall carefully consider the suitability, acceptability and source of the criteria, as described in sections 2.2, 2.3 and 2.4, respectively.

2.1.2 Professionals should consider the selection of criteria carefully. Adhering to local laws and regulations is important and should be considered a mandatory requirement. However it is recognised that many audit 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. The relevance of local and international data protection rules and privacy regulations should be considered. Where legislative requirements are principle-based, professionals should ensure that criteria selected meet the audit objective.

2.1.3 The use of suitable and acceptable criteria is required to ensure a consistent evaluation of the subject matter. Without the right criteria, any conclusion or opinion formed will be open for misunderstanding and interpretability from a personal point of view by the reader.

2.1.4 Professionals should refrain from evaluating the subject matter on the basis of their own expectations, experiences or judgements, because this would not be considered as suitable and acceptable criteria.

2.1.5 Where criteria are not readily available, incomplete or subject to interpretation, professionals should 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 clear.

2.1.6 Professional judgement should be used in ensuring that 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.

2.2 Suitability

2.2.1 Professionals should assess the suitability and appropriateness of the criteria used for assessing subject matter. The example criterion 'Local law stipulates that all personal information of clients should always remain private when conducting data transactions' is used to clarify the following criteria attributes:

- **Objectivity**—Free from bias that may adversely impact professionals' findings and conclusions and, accordingly, may mislead the user of the audit report, e.g., the criterion is objective because it is ratified by local law
- **Completeness**–Sufficiently complete so that all criteria that could affect professionals' conclusions about the subject matter are identified and used in the conduct of the audit engagement. Thus, completeness of all criteria used should be achieved, given the objectives of the audit engagement.
- **Relevance**—Relevant to the subject matter and contribute to findings and conclusions that meet the objectives of the audit engagement. Criteria can be context-sensitive; even for the same subject matter there can be different criteria depending on the objectives and circumstances of the audit engagement, e.g., the criterion is considered relevant because data transactions are in scope of this audit engagement.
- **Measurability**—Permit consistent measurement of the subject matter and the development of consistent conclusions when applied by different professionals in similar circumstances, e.g., the criterion is measurable because every data transaction with unprotected personal information can be uniquely identified and thus consistently measured
- **Understandability**—Communicated clearly and not subject to significantly different interpretations by intended users, e.g., the criterion is understandable because this section of the law has already been the subject of multiple court rulings, helping to establish a clear understanding about the practical execution and interpretation of the law

2008 Criteria *(cont.)*

2.3 Acceptability

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

- **Recognised**—Sufficiently well recognised so that their use is not questioned by intended users
- **Authoritative**—Reflect authoritative pronouncements within the area and are appropriate for the subject matter, e.g., authoritative pronouncements may come from professional bodies, industry groups, government and regulators
- **Publicly available**—Includes standards developed by professional accounting and audit bodies such as ISACA, International Federation of Accountants (IFAC), and other recognised government, legal or professional bodies
- **Available to all users**—Where not publicly available, criteria should be communicated to all users through assertions that form part of the audit report. Assertions consist of statements about the subject matter that meet the requirements of 'suitable criteria' so that they can be audited, as described in Standard 1007 Assertions.

2.3.2 Professionals should ensure that the criteria used in an audit engagement are either:

- **Externally accepted**—Recognised, authoritative and publicly available
- **Externally confirmed**—Criteria developed by management (for a specific audit engagement) are not considered recognised, authoritative and publicly available. Before use, these criteria require external validation by a recognised independent third party to ensure that management does not implicitly enforce a wanted outcome of the audit engagement.

2.4 Source

2.4.1 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**—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 entities that did not follow due process**—These include relevant criteria developed by other entities that did not follow due process and have not been subject to public consultation and debate.
- **Criteria developed specifically for the audit engagement**—While criteria developed specifically for the audit engagement may be appropriate, take particular care to ensure that these criteria are suitable, especially objective, complete and measurable. Criteria developed specifically for an audit engagement are in the form of assertions. They are usually developed to pertain to the needs of a specific user. For example, various frameworks can be used as established criteria for evaluating the effectiveness of the internal control system; a certain user, however, may develop a set of criteria that meets specific needs, e.g., a hierarchy of authorised approvals. Professionals should clearly mention in the audit report that certain criteria are developed specifically for the audit engagement. They should consider if the developed criteria could mislead the intended user and, if required, provide more information on the criteria. Whereas these criteria were developed by management, external confirmation should be sought and mentioned in the report, as described in 2.3.2.

2008 Criteria *(cont.)*

2.5 Change in Criteria During the Audit Engagement

2.5.1 As the audit progresses, additional information and insight on the subject matter may result in a change of selected criteria:
- Certain criteria might not be needed anymore to achieve the audit objective. In these circumstances, further audit work related to the criteria is not necessary.
- There might be a need for extra criteria to achieve the audit objective. In these circumstances, extra criteria will be selected and audit work related to the criteria will be conducted.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1007 Assertions	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	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.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM01 Ensure governance framework setting and maintenance.	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for the board members are met.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

2008 Criteria *(cont.)*

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance, when considered necessary. This could be from IS audit and assurance:

- Colleagues from within the organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

4. Terminology

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.
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.
Professional judgement	The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement
Subject matter	The specific information subject to an IS auditor's report and related procedures, which can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations (area of activity).

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit and assurance engagements beginning on or after 1 September 2014.

Performance Guidelines

The performance guidelines are:
2201 Engagement Planning
2202 Risk Assessment in Audit Planning
2203 Performance and Supervision
2204 Materiality
2205 Evidence
2206 Using the Work of Other Experts
2207 Irregularity and Illegal Acts
2208 Sampling

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

2201 Engagement Planning

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 This guideline provides guidance to the IS audit and assurance professionals. 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, managed and performed in an effective and efficient manner.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1201 Engagement Planning
1.2.2 Standard 1202 Risk Assessment in Audit Planning
1.2.3 Standard 1203 Performance and Supervision
1.2.4 Standard 1204 Materiality

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 IS audit plan
2.2 Objectives
2.3 Scope and business knowledge
2.4 Risk-based approach
2.5 Documenting the audit engagement project plan
2.6 Changes during the course of the audit

2201 Engagement Planning *(cont.)*

2.1 IS Audit Plan

2.1.1 For an audit function, a comprehensive risk-based IS audit plan should be developed and updated, at least annually. A multi-annual (three to five years) time horizon should be established and incorporated into the annual plan. The multi-annual and annual plans should act as a framework for IS audit and assurance activities and serve to address responsibilities set by the audit charter.

2.1.2 The IS audit plan should be prepared so that it is in compliance with any appropriate external requirements in addition to the current ISACA standards. .

2.1.3 Each audit engagement should be referenced either to the IS audit plan or state the specific mandate, objectives and other relevant aspects of the work to be performed.

2.2 Objectives

2.2.1 Professionals should define the audit engagement objectives and document them in the audit engagement project plan, so that they will be performed in an effective manner. The engagement objectives should be established to address the risk associated with the activity under review.

2.2.2 Professionals should develop an audit engagement project plan that takes into consideration the objectives of the audit engagement. These objectives might influence the audit engagement, e.g., resources needed, timeline and deliverables.

2.3 Scope and Business Knowledge

2.3.1 Before beginning an audit engagement, the work of professionals should be planned in a manner appropriate for meeting the audit objectives. As part of the planning process, professionals should obtain an understanding of the enterprise and its processes. This will assist them in determining the significance of the resources being reviewed as they relate to the objectives of the enterprise. In this way, professionals can focus on the areas most sensitive to fraudulent or inaccurate practices. They should establish the scope of the audit work and also perform a preliminary assessment of the internal controls over the function being reviewed.

2.3.2 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 audit engagement. Knowledge of the enterprise should include the business and financial risk facing the enterprise as well as conditions in the enterprise marketplace and the extent to which the enterprise relies on outsourcing to meet its objectives. 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.

2.4 Risk-based Approach

2.4.1 Professionals should develop an audit engagement project plan to reduce audit risk to an acceptable level.

2.4.2 A risk assessment should be performed to provide reasonable assurance that all material items will be covered adequately during the audit engagement and that professionals will be able to come to a conclusion. This assessment should identify areas with relatively high probability of material problems.

2.4.3 A risk assessment and prioritisation of identified risk for the area under review and the enterprise IS environment should be carried out to the extent necessary.

2.4.4 Normally in the planning process, professionals should 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, professionals should evaluate materiality of the various components of the system in planning the audit engagement for the work to be performed. Both qualitative and quantitative aspects should be considered in determining materiality.

2.4.5 Before beginning an audit engagement and in the course of the audit, the professionals should consider compliance with applicable laws and professional auditing standards.

2.4.6 When professionals evaluate internal controls for the purpose of placing reliance on control procedures in support of information being gathered as part of a larger audit exercise (such as an audit of historical financial information), they should, as a rule, make a preliminary evaluation of the controls and develop the audit engagement project plan on the basis of this evaluation.

2201 Engagement Planning *(cont.)*

2.5 Documenting the Audit Engagement Project Plan

2.5.1 Professionals' work papers should include the audit engagement project plan.

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

- Areas to be audited
- Type of work planned
- High-level objectives and scope of the work
- Fact-finding interviews to be conducted
- Relevant information to be obtained
- Procedures to verify or validate the information obtained and their use as audit evidence
- General topics, e.g.:
  - Budget
  - Resource availability and allocation
  - Schedule dates
  - Type of report
  - Intended audience
  - Deliverables
- Specific topics, e.g.:
  - Identification of tools needed for gathering evidence, performing tests and preparing/summarising information for reporting
  - Assessment criteria to be used
  - Reporting requirements and distribution
- Other general aspects of the work, when applicable

2.5.3 The project plan should include the requirements related to the timeline of the audit engagement, such as the period covered and the different completion dates, to perform the audit engagement within the agreed-on schedule. This also includes budgetary expenditure.

2.5.4 Professionals should ensure full coverage of the required competencies by the resources of the audit engagement. They should set up an audit engagement team that has the right skills, knowledge and experience to successfully complete the audit engagement. The professionals should make sure to assign the different roles and responsibilities to the IS audit team members that best match with their competencies. For more information refer to Standard 1203 Performance and Supervision.

2.5.5 The audit engagement project plan should list all deliverables that are linked to the audit engagement.

2.5.6 The audit engagement project plan and any subsequent changes to this plan should be approved by the IS audit and assurance management.

2.5.7 After approval by the IS audit and assurance management, parts of the audit engagement project plan (e.g., scope, timeline, document requirements, interview schedule) should be timely communicated towards the auditees for them to provide appropriate and complete access and availability to the needed documents and resources.

2.6 Changes During the Course of the Audit

2.6.1 The audit engagement project plan should be updated and changed as necessary during the course of the audit engagement.

2.6.2 Planning an audit engagement is a continual and iterative process. As a result of unexpected events, changes in conditions or the audit evidence obtained, professionals may need to modify the planned nature, timing and extent of further audit procedures.

2.6.3 The audit plan should consider the possibility of unexpected events that imply risk for the enterprise. Accordingly, the audit engagement project plan should be able to prioritise such events within the audit and assurance processes based on risk.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:

3.1 Linkage to standards

3.2 Linkage to COBIT 5 processes

3.3 Other guidance

2201 Engagement Planning *(cont.)*

3.1 Linkage to Standards

The table provides an overview of:

- The most relevant ISACA standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1201 Engagement Planning	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 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 Audit Planning	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. IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements.
1203 Performance and Supervision	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.
1204 Materiality	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.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:

- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
MEA01 Monitor, evaluate and assess performance and conformance.	Provide transparency of performance and conformance and drive achievement of goals.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

2201 Engagement Planning *(cont.)*

3.3 Other Guidance When implementing standards and guidelines, professionals are encouraged to seek other guidance, when considered necessary. This could be from IS audit and assurance:

- Colleagues from within the organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Audit plan	1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion. Scope Notes: Includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work 2. A high-level description of the audit work to be performed in a certain period of time.
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
Materiality	An audit concept regarding the importance of an item of information with regard to its impact or effect on the subject matter being audited. An expression of the relative significance or importance of a particular matter in the context of the engagement or 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.

5. Effective Date

5.1 Effective Date This revised guideline is effective for all IS audit and assurance engagements beginning on or after 1 September 2014.

2202 Risk Assessment and Audit Planning

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The level of audit work required to meet the audit objective is a subjective decision made by IS audit and assurance professionals. The purpose of this guideline is to reduce the risk of reaching an incorrect conclusion based on the audit findings and to reduce the existence of errors in the area being audited.

1.1.2 The guideline provides guidance in applying a risk assessment approach to develop an:
- IS audit plan that covers all annual audit engagements
- Audit engagement project plan that focuses on one specific audit engagement

1.1.3 The guideline provides the details of the different types of risk the IS audit and assurance professionals encounter.

1.1.4 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1201 Engagement Planning
1.2.2 Standard 1202 Risk Assessment in Planning
1.2.3 Standard 1203 Performance and Supervision
1.2.4 Standard 1204 Materiality
1.2.5 Standard 1207 Irregularity and Illegal Acts

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Risk assessment of the IS audit plan
2.2 Risk assessment methodology
2.3 Risk assessment of individual audit engagements
2.4 Audit risk
2.5 Inherent risk
2.6 Control risk
2.7 Detection risk

2202 Risk Assessment and Audit Planning *(cont.)*

2.1 Risk Assessment of the IS Audit Plan

2.1.1 When developing the overall IS audit plan, a suitable risk assessment approach should be followed. A risk assessment should be conducted and documented at least annually to facilitate the development process of the IS audit plan. It should take into account the organisational strategic plans and objectives and the enterprise risk management framework and initiatives.

2.1.2 To correctly and completely assess the risk that is related to the complete scope of the IS audit area, professionals should consider the following elements when developing the IS audit plan:
- Full coverage of all areas within the scope of the IS audit universe, which represents the range of all possible audit activities
- Reliability and suitability of the risk assessment provided by management
- The processes followed by management to supervise, examine and report possible risk or issues
- Cover risk in related activities relevant to the activities under review

2.1.3 The applied risk assessment approach should help with the prioritisation and scheduling process of the IS audit and assurance work. It should support the selection of areas and items of audit interest and the decision process to design and conduct particular IS audit engagements.

2.1.4 Professionals should ensure that the applied risk assessment approach is approved by those charged with governance and distributed to the various engagement stakeholders

2.1.5 Professionals should use risk assessments to quantify and justify the amount of IS audit resources needed to complete the IS audit plan and the requirements for specific engagements

2.1.6 Based on the risk assessment(s), professionals should develop an IS audit plan that acts as a framework for the IS audit and assurance activities. It should:
- Consider non-IS audit and assurance requirements and activities
- Be updated at least annually
- Be approved by those charged with governance
- Address responsibilities set by the audit charter

For more information refer to Standard 1201 Engagement Planning.

2.2 Risk Assessment Methodology

2.2.1 Professionals should consider the appropriate risk assessment methodology to ensure complete and accurate coverage of the audit engagements in the IS audit plan.

2.2.2 Professionals should at least include an analysis, within the methodology, of the risk to the enterprise related to system availability, data integrity and business information confidentiality.

2.2.3 Many risk assessment methodologies are available to support the risk assessment process. These range from simple classifications of high, medium and low, based on professionals' judgement, to more quantitative and scientific calculations providing a numeric risk rating, and others which are a combination of the two. Professionals should consider the level of complexity and detail appropriate for the enterprise or subject(s) being audited. Specific guidance on performing risk assessments can be found in the ISACA publication *COBIT 5 for Risk*.

2.2.4 All risk assessment methodologies rely on subjective judgements at some point in the process (e.g., for assigning weights to the various parameters). Professionals 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.

2.2.5 In deciding which is the most appropriate risk assessment methodology, professionals 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 audit engagements)
- Cost of software or other licences required to use the methodology
- Extent to which the information required is already available
- 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)
- 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
- Willingness of those charged with governance of the IS audit area to accept the methodology as the means of determining the type and level of audit work carried out

2202 Risk Assessment and Audit Planning *(cont.)*

2.2 Risk Assessment Methodology (cont.)

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

2.2.7 The professionals should use the selected risk assessment techniques in developing the overall IS audit plan and in planning specific audit engagements. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as the:
- Areas or business functions to be audited
- Amount of time and resources to be allocated to an audit
- Nature, extent and timing of audit procedures

2.2.8 The risk assessment methodologies adopted should produce consistent, valid, comparable and repeatable results. Risk assessments that come out of the methodology should be consistent (over a period), valid, comparable (with earlier/later assessments using the same assessment methodology) and repeatable (given a similar set of facts, using the same assessment methodology will produce a similar outcome).

2.3 Risk Assessment of Individual Audit Engagements

2.3.1 When planning an individual engagement, professionals should identify and assess risk relevant to the area under review. The results of this risk assessment should be reflected in the audit engagement objectives. During the risk assessment, professionals should consider:
- Results of prior audit engagements, reviews and findings, including any remedial activities
- The enterprise overarching risk assessment process
- The likelihood of occurrence of a particular risk
- The impact of a particular risk (in monetary or other value measures) if it occurs

2.3.2 Professionals should ensure full understanding of the activities in scope before assessing risk. They should request comments and suggestions from stakeholders and other appropriate parties. This is needed to correctly determine and examine the impact of possible risk in the audit engagements.

2.3.3 The goal of the risk assessment is the reduction of audit risk to an acceptably low level, and identifying those parts of an activity that should receive more audit focus. This needs to be performed by an appropriate assessment of the IS subject matter and related controls, while planning and performing the IS audit.

2.3.4 When planning a specific IS audit and assurance procedure, professionals should recognise the fact that the lower the materiality threshold is, the more precise the audit expectations will be and the greater the audit risk.

2.3.5 When planning a specific IS audit and assurance procedure, professionals should consider possible illegal acts that can require a modification of the nature, timing or extent of the existing procedures. For more information refer to Standard 1207 Irregularity and Illegal Acts and Guideline 2207.

2.3.6 To gain additional assurance in instances where there is high audit risk or a lower materiality threshold, professionals should compensate by either extending the scope or nature of the IS audit tests or increasing or extending the substantive testing.

2.4 Audit Risk

2.4.1 Audit risk refers to the risk of reaching an incorrect conclusion based upon audit findings. The three components of audit risk are:
- Control risk
- Detection risk
- Inherent risk

2.4.2 Professionals should consider each of the risk components to determine the overall level of risk. This includes subject matter risk, which includes inherent risk and control risk; together with detection risk it is then referred to as audit risk. Further elaboration on the different components of audit risk can be found in sections 2.5 to 2.7.

2202 Risk Assessment and Audit Planning *(cont.)*

2.5 Inherent Risk

2.5.1 Inherent risk is the susceptibility of an audit area to err 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 systems without appropriate controls 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 without controls, when a proper analysis demonstrates it is not used for business-critical purposes, ordinarily is low.

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

2.6 Control Risk

2.6.1 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 of the volume of logged information. The control risk associated with computerised data validation procedures ordinarily is low because the processes are applied consistently.

2.6.2 Professionals should assess the control risk as high unless relevant internal controls are:
- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

2.6.3 The professionals should consider both pervasive and detailed IS controls:
- Pervasive IS controls are considered a subset of general controls; they are those general controls that focus on the management and monitoring of the IS environment. They therefore affect all IS-related activities. The effect of pervasive IS controls on professionals' work is not limited to the reliability of application controls in the business process systems. They also affect the reliability of the detailed IS controls over, e.g., application program development, system implementation, security administration and backup procedures. Weak pervasive IS controls, and thus weak management and monitoring of the IS environment, should alert professionals to the possibility of a high risk that the controls designed to operate at the detailed level may be ineffective.
- Detailed IS controls are made up of application controls plus those general controls not included in pervasive IS controls. Following the COBIT framework, they are the controls over the acquisition, implementation, delivery and support of IS systems and services.

2.6.4 A risk that professionals should consider is the limitations and shortcomings in the detailed IS controls that are induced by inadequacies of the pervasive IS controls.

2.7 Detection Risk

2.7.1 Detection risk is the risk that professionals' 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 ordinarily is 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 ordinarily is low, since existence is verified easily.

2.7.2 In determining the level of substantive testing required, the professionals should consider the:
- Assessment of inherent risk
- Conclusion reached on control risk following compliance testing

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

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

2202 Risk Assessment and Audit Planning *(cont.)*

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA Standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1201 Engagement Planning	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
1202 Risk Assessment in Planning	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. IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements. IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.
1203 Performance and Supervision	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.
1204 Materiality	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. IS audit and assurance professionals shall consider materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures. 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. IS audit and assurance professionals shall disclose the following in the report: • Absence of controls or ineffective controls • Significance of the control deficiencies • Likelihood of these weaknesses resulting in a significant deficiency or material weakness
1207 Irregularity and Illegal Acts	IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement.

2202 Risk Assessment and Audit Planning *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM01 Ensure governance framework setting and maintenance.	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.
EDM03 Ensure risk optimisation.	Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
APO12 Manage risk.	Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance, when considered necessary. This could be from IS audit and assurance:
- Colleagues from within the organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

2202 Risk Assessment and Audit Planning *(cont.)*

4. Terminology

Term	Definition
Audit charter	A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal IS audit and assurance activity
	The charter should: • Establish the internal IS audit and assurance 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 IS audit and assurance function's activities
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
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.
Detailed IS controls	Controls over the acquisition, implementation, delivery and support of IS systems and services made up of application controls plus those general controls not included in pervasive controls
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 subject matter being audited. An expression of the relative significance or importance of a particular matter in the context of the engagement or 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.
Pervasive IS control	General control designed to manage and monitor the IS environment and which, therefore, affects all IS-related activities
Substantive testing	Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period

5. Effective Date

5.1 Effective Date This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2203 Performance and Supervision

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 This guideline provides guidance to IS audit and assurance professionals in performing the audit engagement and supervising IS audit team members. It covers:
- Performing an audit engagement
- Roles and responsibilities, required knowledge, and skills for performing audit engagements
- Key aspects of supervision
- Gathering evidence
- Documenting work performed
- Formulating findings and conclusions

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1005 Due Professional Care
1.2.2 Standard 1006 Proficiency
1.2.3 Standard 1201 Engagement Planning
1.2.4 Standard 1203 Performance and Supervision
1.2.5 Standard 1205 Evidence
1.2.6 Standard 1401 Reporting

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Performing the work
2.2 Roles and responsibilities, knowledge and skills
2.3 Supervision
2.4 Evidence
2.5 Documenting
2.6 Findings and conclusions

2203 Performance and Supervision *(cont.)*

2.1 Performing the Work

2.1.1 Professionals shall plan and perform each audit engagement in accordance with the approved IS audit plan. Setting up an audit engagement project plan, as detailed in Standard 1201 Engagement Planning, allows professionals to understand all elements in scope, the required skills and knowledge to execute the audit engagement within the agreed-on schedule, while covering all identified risk.

2.1.2 The main tasks in performing an audit engagement include:

- **Planning and risk assessment**—Professionals should conduct these activities in alignment with standards 1201 Engagement Planning and 1202 Risk Assessment in Planning.
- **Identifying controls**—Based on the scope, audit objectives and main areas of risk identified in the IS audit plan, professionals should identify the controls in scope of the audit engagement.
- **Assessing controls and gathering evidence**—Professionals should assess the controls in scope by gathering and analysing information and evidence on the design effectiveness and operating effectiveness of the controls, as described in Standard 1205 Evidence.
- **Documenting work performed and identifying findings**—Professionals should document the work performed, record the information and evidence gathered and document any identified findings.
- **Confirming findings and following up on corrective actions**—Professionals should confirm their findings with the auditee. Should the auditee perform corrective actions on the findings before the end of the audit engagement, professionals should include the actions taken in the documentation (and conclusion), but should also always mention the original findings.
- **Drawing conclusions and reporting**—Professionals should draw conclusions and report about the impact of the findings on achieving the audit objectives, as detailed in Standard 1401 Reporting. Focusing only on the control findings, without assessing the impact on the audit objectives, is insufficient.

2.2 Roles and Responsibilities, Knowledge and Skills

2.2.1 Professionals in charge of the audit engagement should define and manage the roles and responsibilities of the IS audit team members throughout the engagement, addressing at a minimum:

- Designing the methodology and approach
- Creating audit work programmes
- Defining execution and review roles
- Dealing with issues, concerns and problems as they arise
- Documenting and clearing the findings
- Writing the report

2.2.2 Based on the engagement needs, professionals in charge should consider the required competencies for the specific audit engagement. They should set up an engagement team that has the combined skills, knowledge and experience to complete the audit engagement successfully. Professionals should make sure to assign those roles and responsibilities to the IS audit team members that best match their competencies.

2.2.3 Professionals should only accept roles, responsibilities and associated tasks that are within their knowledge and skills. Time and cost issues might prohibit professionals from acquiring all of the necessary knowledge and skills before the start of an audit engagement; therefore, professionals are allowed to accept roles, responsibilities and associated tasks if they have reasonable expectation that appropriate measures will be taken during the audit engagement to ensure successful completion. The following measures would allow for such a reasonable expectation:

- **Learning on the job**—In certain circumstances, it will be possible for professionals to acquire the necessary skills and knowledge during the audit engagement.
- **Supervision**—Professionals in charge could arrange for adequate supervision of the IS audit team members, allowing them to successfully achieve the task under supervision.
- **External resources**—Professionals in charge could consider hiring external experts for those areas of the audit engagement that are lacking adequate internal knowledge and skills. Professionals in charge should consider promoting the development of internal IS audit team members by having them work closely with the external expert to assure a transfer of knowledge and skills to the team.

2.2.4 Guidance on acquiring, maintaining and monitoring required competencies is detailed in Standard 1006 Proficiency.

2203 Performance and Supervision *(cont.)*

2.3 Supervision

2.3.1 Every task executed during an audit engagement by the IS audit team members should be supervised by professionals that have supervisory responsibilities over them, to ensure that audit objectives and applicable professional audit standards are met. The extent of supervision required will highly depend on the skills, knowledge and experience of professionals executing the task under review and on the complexity of the audit engagement.

2.3.2 Supervision is a process that is present in every step of the audit engagement. This includes:
- Ensuring the IS audit team members have the combined skills, knowledge and experience to complete the audit engagement successfully
- Ensuring an appropriate audit engagement project plan and audit work programme is set up and approved
- Reviewing the audit engagement work papers
- Ensuring audit engagement communication toward auditees and other relevant stakeholders is accurate, clear, concise, objective, constructive and timely
- Ensuring that the approved audit engagement work programme is completed at the end of the audit engagement, unless changes were justified and approved beforehand, and the audit engagement objectives are met
- Providing opportunities for IS audit team members to develop their skills and knowledge

2.3.3 Reviewing audit engagement work papers is required to ensure that all necessary audit procedures are performed, evidence gathered is sufficient and appropriate, and conclusions adequately support the engagement objectives and conclusion or opinion. Considering the objective of the review, this should be performed by IS audit team members having supervisory responsibilities over professionals who created the audit engagement work papers.

2.3.4 During the review process, reviewers should record questions as they arise. When professionals provide an answer or solution to questions raised, care should be taken to ensure that sufficient and appropriate evidence is retained to show that questions were raised, treated and answered.

2.3.5 Appropriate evidence of review should be documented and retained. Options to document evidence of performing a review consist of, but are not limited to:
- Signing and dating each audit engagement work paper after review
- Completing an audit engagement work paper review checklist
- Preparing a signed document that provides a reference to the audit engagement work papers under review and detail the nature, timing, extent and result of the review

All of these options are valid both electronically and on hard copy.

2.3.6 Supervision allows for development and performance evaluation of professionals. Reviewers have a privileged view of the work performed by other IS audit team members, which allows for a detailed and adequate evaluation of their performance. The reviewers should point out areas of development and advise on ways to improve skills and knowledge.

2.4 Evidence

2.4.1 Professionals should obtain evidence that is sufficient and appropriate to form an opinion or support the conclusions and achieve the audit objectives. Determining whether evidence is sufficient and appropriate should be based on the importance of the audit objective and the effort involved in obtaining the evidence.

2.4.2 Professionals should obtain additional evidence if, in their judgement, the evidence obtained does not meet the criteria of being sufficient and appropriate to form an opinion or support the conclusions and achieve the audit objectives.

2.4.3 Professionals should select the most appropriate procedure to gather evidence, depending on the subject matter being audited.

2.4.4 Professionals should consider the source and nature of evidence obtained to evaluate its reliability and the need for further verification.

2203 Performance and Supervision *(cont.)*

2.4 Evidence (cont.)

2.4.5 Appropriate analysis and interpretation should be performed by professionals to support the audit findings and form conclusions. Evidence and information received should be compared with expectations identified or developed by professionals. Professionals should be aware of:
- Unexpected differences
- The absence of differences when they were expected
- Potential errors
- Fraud or illegal acts
- Non-compliance with laws or regulations
- Unusual or nonrecurring activities

2.4.6 Should deviations from expectations be identified, professionals should ask management about the reasons for the difference. Should management's explanation be adequate, according to professional judgement, professionals should modify their expectations and re-analyse the evidence and information.

2.4.7 Significant deviations not adequately explained by the auditee should result in audit findings and be communicated to executive management or those charged with governance. Depending on the circumstances, professionals could recommend appropriate action to be taken.

2.4.8 Detailed guidance on the different kinds of evidence, procedures to collect evidence, applicable sources, ways to assess evidence, etc., can be found in Standard 1205 Evidence.

2.5 Documenting

2.5.1 Professionals should prepare sufficient, appropriate and relevant documentation in a timely manner that provides a basis for the conclusion and contains evidence of the review performed. Sufficient, appropriate and relevant documentation should enable a prudent and informed person, with no previous connection to the audit engagement, to re-perform the tasks performed during the audit engagement and reach the same conclusion. Documentation should include:
- Audit engagement objectives and scope of work
- Audit engagement project plan
- Audit work programme
- Audit steps performed
- Evidence gathered
- Conclusions and recommendations

2.5.2 Documentation aids in planning, performing and reviewing audit engagements because it:
- Identifies who of the IS audit team members performed each audit task and their role in preparing and reviewing the documentation
- Records the evidences requested
- Supports the accuracy, completeness and validity of the work performed
- Provides support for the conclusions reached
- Facilitates the review process
- Documents whether the engagement objectives were reached
- Provides the basis for quality improvement programmes

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

2.5.4 Performance and supervision activities should be documented in audit engagement work papers. The design and content of the audit engagement work papers varies depending on the circumstances of the particular audit engagement. IS audit and assurance management, however, should detail a limited number of standard template work papers for different types of audit engagements. Standard work papers improve the efficiency of the audit engagement and facilitate supervision. IS audit and assurance management should also determine the media carriers to be used, and storage and retention procedures for the work papers.

2.5.5 Professionals should ensure that documentation of the work performed is completed on a timely basis. All information and evidence required to form a conclusion or opinion should be obtained prior to the issue date of the audit report. Audit engagement work papers should include the date they were prepared and reviewed.

2.5.6 Audit engagement work papers are the property of the enterprise. IS audit and assurance management controls the work papers and provides access to authorised personnel. Access requests to audit engagement work papers by external auditors should be approved by executive management and those charged with governance. Access requests by external parties, other than external auditors, should be approved by executive management and those charged with governance, and advised by legal counsel.

2203 Performance and Supervision *(cont.)*

2.6 Findings and Conclusions

2.6.1 Professionals should analyse the evidence and information gathered, as described in section 2.4.5. Significant deviations from expectation should result in findings. Professionals should confirm these findings with the auditee, as well as the impact of these findings on other aspects of the control environment.

2.6.2 Professionals can propose corrective actions to be taken, but will never execute them. Should the auditee perform corrective actions that remediate the original finding, before the end of the audit engagement, professionals should include the corrective actions taken in the documentation.

2.6.3 Professionals should conclude on the findings identified and assess their impact on the audit objectives. Conclusions should be formed on the original findings. If corrective actions have been performed, an addendum to the conclusion can be formulated explaining the corrective action and the impact of the corrective action on the original conclusion.

2.6.4 All the conclusions formulated and whether or not the audit objectives have been achieved should be documented in the audit engagement report. Detailed guidance on reporting can be found in Standard 1401 Reporting and Guideline 2401 Reporting.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA Standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1005 Due Professional Care	IS audit and assurance professionals shall exercise due care, including observance of applicable professional audit standards, in planning, performing and reporting on the results of IS audit or assurance engagements.
1006 Proficiency	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. IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate knowledge of the subject matter.
1201 Engagement Planning	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 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

2203 Performance and Supervision *(cont.)*

3.1 Linkage to Standards (cont.)

Standard Title	Relevant Standard Statements
1203 Performance and Supervision	IS audit and assurance professional shall conduct the work in accordance with the approved IS audit plan to cover identified risk and within the agreed-on schedule. 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. 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. IS audit and assurance professionals shall obtain sufficient, reliable, relevant and timely evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence. IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions. IS audit and assurance professionals shall identify and conclude on findings.
1205 Evidence	IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. IS audit and assurance professionals shall evaluate the sufficiency of audit evidence obtained to support conclusions and achieve IS audit or assurance engagement objectives.
1401 Reporting	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. IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient and appropriate audit evidence.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
APO07 Manage human resources.	Optimise human resources capabilities to meet enterprise objectives.
APO08 Manage relationships.	Create improved outcomes, increased confidence, trust in IT and effective use of resources.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

2203 Performance and Supervision *(cont.)*

3.3 Other Guidance When implementing standards and guidelines, professionals are encouraged to seek other guidance, when considered necessary. This could be from IS audit and assurance:

- Colleagues from within the organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Control environment	The attitude and actions of the board and management regarding the significance of control within the organisation. The control environment provides discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements: • Integrity and ethical values • Management philosophy and operating style • Organizational structure • Assignment of authority and responsibility • Human resource policies and practices • Competence of personnel Source: International Standards for the Professional Practice of Internal Auditing, 2010
Design effectiveness	If the company's controls are operated as prescribed by persons possessing the necessary authority and competence to perform the control effectively, satisfy the company's control objectives and can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements, they are considered to be designed effectively. Source: PCAOB, Auditing Standard No. 5, 2007
Operating effectiveness	If a control is operating as designed and the person performing the control possesses the necessary authority and competence to perform the control effectively, the control is considered to be operating effectively. Source: PCAOB, Auditing Standard No. 5, 2007

5. Effective Date

5.1 Effective Date This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2204 Materiality

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to clearly define the concept 'materiality' for the IS audit and assurance professionals and make a clear distinction with the materiality concept used by financial audit and assurance professionals.

1.1.2 The guideline assists the IS audit and assurance professionals in assessing materiality of the subject matter and considering materiality in relationship to controls and reportable issues.

1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1201 Engagement Planning
1.2.2 Standard 1202 Risk Assessment in Planning
1.2.3 Standard 1204 Materiality
1.2.4 Standard 1207 Irregularity and Illegal Acts

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 IS vs. financial audit engagements
2.2 Assessing materiality of the subject matter
2.3 Materiality and controls
2.4 Materiality and reportable issues

2.1 IS vs. Financial Audit Engagements

2.1.1 IS professionals require a different yardstick to measure materiality, as compared to their colleagues working on financial audit engagements. Financial professionals normally measure materiality in monetary terms, because what they audit is also measured and reported in monetary terms. IS professionals normally perform audits of non-financial items, e.g., program development controls, program change controls, physical access controls, logical access controls and computer operation controls on a variety of systems. Therefore, IS professionals may need guidance on how materiality should be assessed to plan their audit engagements effectively, how to focus their efforts on high-risk areas and how to assess the severity of any errors or weaknesses found.

2204 Materiality *(cont.)*

2.2 Assessing Materiality of the Subject Matter

2.2.1 The assessment of what is material is a matter of professional judgement. It includes consideration of the effect and/or the potential effect on the enterprise'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. Where the IS audit objective relates to systems or operations that process financial transactions, the financial professional's measure of materiality should be considered while conducting the IS audit.

2.2.2 To assess materiality, professionals should establish a classification of information assets in terms of:
- Confidentiality, availability and integrity
- Access control rules on privileges management
- Degree of criticality and risk to the business
- Compliance with laws and regulations

The assessment should include consideration of:
- The nature of data and information processed and stored
- IS hardware
- IS architecture and software (applications and operating systems)
- IS network infrastructure
- IS operations
- Production, development and test environments
- Applicable laws and regulations

2.2.3 More detailed examples of factors that could be considered to assess materiality are:
- 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 applications developed
- Number of users who use the information system
- Number of managers and directors who work with the information system 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, overhead or any 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, but also loss of reputation and image
- 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 health, safety and environmental requirements
- Specific definitions of, or considerations about, materiality provided by legislative or regulatory authorities
- Transfer of IT operations to a third party, which causes a significant change in compliance regulatory requirements, e.g., data privacy and protection, trade control rules, financial requirements

2.2.4 The indication of higher importance subject areas should be used to reduce audit risk appropriately by either extending the test of controls (reduce control risk) and/or extending the substantive testing procedures (reduce detection risk).

2.2.5 Professionals should re-evaluate established materiality when changes in particular circumstances or additional information come to their attention that might influence materiality of systems or operations. The most common situations in which this could happen include:
- Materiality was established initially on estimations or on preliminary information that differs significantly from the actual situation.
- Events or changes in conditions since materiality was set have a significant impact on the ability of the enterprise to meet its business objectives.

2204 Materiality *(cont.)*

2.3 Materiality and Controls

2.3.1 To meet the audit objectives, professionals should identify the relevant control objectives and, based on the risk tolerance level, determine what should be examined. With respect to a specific control objective, a control or group of controls is material if the absence of the control results in failure to provide reasonable assurance that the control objective will be met.

2.3.2 Professionals should consider materiality when determining the nature, timing and extent of the audit procedures to be applied to test a control or group of controls. Material controls should be tested more thoroughly, frequently and extensively compared to non-material controls to reduce the audit risk.

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

2.3.4 Before the start of the audit engagement field work, professionals should consider obtaining sign-off from appropriate stakeholders acknowledging that any existing material weakness that stakeholders are aware of in the enterprise has been disclosed.

2.3.5 When professionals discover control deficiencies, they should evaluate the effect on the overall audit opinion or conclusion. When evaluating the effect, professionals should take into account different aspects of the occurrence of the control deficiencies, including:
- Size
- Nature
- Particular circumstances

2.3.6 When testing material controls, professionals should evaluate the effect of compensating controls in mitigating risk associated with a discovered control deficiency. The control deficiency should be classified as:
- A material weakness, when the compensating controls are ineffective
- A significant deficiency, when the compensating controls are partially effective
- An inconsequential deficiency, when the compensating controls reduce the risk to an acceptable level

2.3.7 Multiple errors or control failures might cause a cumulative effect, which professionals should consider in determining the overall materiality of control deficiencies.

2.3.8 Professionals should determine whether any IT general control deficiency is 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 it is 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.

2.3.9 Professionals 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.

2.3.10 Professionals should also note that failure to remediate a deficiency could become material, e.g., after management and those charged with governance have been alerted to the deficiency.

2.3.11 Control deficiencies are always material in areas where they have been overridden resulting in fraud or illegal acts.

2.4 Materiality and Reportable Issues

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

2.4.2 Where the audit engagement 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.

2.4.3 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 engagement work identifies material control weaknesses, professionals should consider issuing a qualified or adverse opinion on the audit objective.

2.4.4 Depending on the objectives of the audit engagement, professionals should consider reporting to management weaknesses that are not material, particularly when the cost of strengthening the controls is low. In addition, professionals could advise on resolutions for the weaknesses identified.

2204 Materiality *(cont.)*

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA Standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1201 Engagement Planning	IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the: a. Engagement nature, objectives, timeline and resource requirements • Timing and extent of audit procedures to complete the engagement
1202 Risk Assessment In Planning	IS audit and assurance professionals shall identify and assess risk relevant to the area under review when planning individual engagements. IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.
1204 Materiality	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. 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. 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. IS audit and assurance professionals shall disclose the following in the report: • Absence of controls or ineffective controls • Significance of the control deficiencies • Likelihood of these weaknesses resulting in a significant deficiency or material weakness
1207 Irregularity and Illegal Acts	IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement. IS audit and assurance professionals shall maintain an attitude of professional scepticism during the engagement. IS audit and assurance professionals shall document and communicate any material irregularities or illegal act to the appropriate party in a timely manner.

2204 Materiality *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM03 Ensure risk optimisation.	Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance, when considered necessary. This could be from IS audit and assurance:
- Colleagues from within the organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

2204 Materiality *(cont.)*

4. Terminology

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.
Materiality	An audit concept regarding the importance of an item of information with regard to its impact or effect on the subject matter being audited. An expression of the relative significance or importance of a particular matter in the context of the engagement or the enterprise as a whole.
Significant deficiency	A deficiency or a combination of deficiencies, in internal control, that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight Note: A material weakness is a significant deficiency or a combination of significant deficiencies that results in more than a remote likelihood of an undesirable event(s) not being prevented or detected.

5. Effective Date

5.1 Effective Date This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2205 Evidence

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to provide guidance to IS audit and assurance professionals in obtaining sufficient and appropriate evidence, evaluating the received evidence and preparing appropriate audit documentation.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1203 Performance and Supervision
1.2.2 Standard 1205 Evidence
1.2.3 Standard 1206 Using the Work of Other Experts

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Types of evidence
2.2 Obtaining evidence
2.3 Evaluating evidence
2.4 Preparing audit documentation

2205 Evidence *(cont.)*

2.1 Types of Evidence

2.1.1 When planning and performing an engagement, professionals should consider the types of evidence to be gathered, its use to meet engagement objectives, and its varying levels of reliability. The various types of evidence that professionals should consider using include:
- Observed processes and existence of physical items
- Documentary evidence
- Representations
- Analysis

2.1.2 Observed processes and existence of physical items can include observations of activities, property and IS functions, such as:
- A network security monitoring system in operation
- An inventory of media in an offsite storage location

2.1.3 Documentary evidence, recorded on paper or other media, can include:
- Written policies and procedures
- Results of data extractions
- Records of transactions
- Programme listings
- Other documents and records produced in the ordinary course of business

2.1.4 Written and oral representations of those being audited can include:
- Written statement by management, e.g., representations about the existence and effectiveness of internal controls or plans for a new financial system implementation
- Oral representation of such things as how a process works or plans for management follow up on actions related to the security awareness programme

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

2.2 Obtaining Evidence

2.2.1 Professional should obtain sufficient and appropriate evidence to allow them to draw reasonable audit conclusions. This evidence includes:
- The procedures performed
- The results of the procedures performed
- Source documents (in either electronic or paper format), records and corroborating information used to support the audit engagement
- Documentation that the work was performed and complies with applicable laws, regulations and policies

2.2.2 Where evidence obtained in the form of oral representations is critical to the audit opinion or conclusion, professionals should consider obtaining confirmation of the representations, either in writing or electronically (such as through email). Professionals should also consider alternative evidence to corroborate these representations to ensure their reliability.

2.2.3 When gathering evidence, the professional should consider the following:
- The time, level of effort and cost of obtaining the evidence compared to the sufficiency of the evidence in reducing audit risk
- Significance of the matter being evaluated and of the audit procedure requiring the evidence in achieving the audit objectives and reducing audit risk
- Electronic evidence may not be retrievable in whole or in part after the passage of time

2205 Evidence *(cont.)*

2.2 Obtaining Evidence (cont.)

2.2.4 Procedures used to gather evidence vary depending on the characteristics of the information system being audited, timing of the audit, audit scope and objectives, and professional judgement. Evidence can be gathered through the use of manual audit procedures, computer-assisted audit techniques (CAATs) or a combination of both. Professionals should select the most appropriate procedure in relation to the IS audit objective. The following procedures should be considered:

- **Inquiry and confirmation**—The process of seeking information from experienced people who are familiar with the subject matter. The experienced people need not be members of the enterprise being audited. This procedure can range from formal written inquiries to informal oral inquiries.
- **Observation**—Observing a procedure or process being performed by those individuals who are typically responsible for its performance, or observing physical items such as facilities, computer hardware, or information system settings or configurations. This type of evidence is limited to the point in time at which the observation took place. Professionals should take into account that observing the performance of a process or procedure may affect how the procedure or process is being performed.
- **Inspection**—Examination of internal or external documents and records. The items to be inspected can be supplied in paper or electronic form. Inspection can also include physical asset examination.
- **Analytical procedures**—Evaluating (financial or non-financial) data by examining possible relationships within the data or between the data and other relevant information. This also includes the examination of fluctuations, trends and inconsistent relationships.
- **Recalculation/computation**—The process of checking the arithmetical and mathematical accuracy of documents or records. This can be performed manually or through the use of CAATs.
- **Reperformance**—Independent performance of procedures and/or controls that were originally executed by the information system or by the enterprise itself.
- **Other generally accepted methods**—Other generally accepted procedures that can be followed by professionals in gathering sufficient and appropriate evidence. For example, professionals can perform social engineering, act as a mystery guest or conduct ethical intrusion testing.

2.2.5 When gathering evidence, professionals should consider 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 obtained from the enterprise being audited. Physical audit evidence is generally more reliable than the representations of an individual.

2.2.6 If there is a possibility that the gathered evidence will become part of a legal proceeding, professionals 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.

2.2.7 In situations where professionals are not able to obtain sufficient audit evidence, such as when individuals or management refuse to provide sufficient and appropriate evidence necessary to achieve the IS audit objectives, professionals should disclose this situation to audit management, and if necessary to those charged with governance. Professionals should also disclose this fact in accordance with the audit organisation's established procedures. Restriction or limitations on the scope of the audit and achievement of the audit objectives should also be disclosed in the communication of the audit results.

2.2.8 Professionals should retain evidence after completion of the audit work to ensure that the evidence is:

- Available for a time period and in a format that complies with the audit 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

2205 Evidence *(cont.)*

2.3 Evaluating Evidence

2.3.1 Evidence is sufficient and appropriate when it provides a reasonable basis for supporting the findings or conclusions within the context of the audit objectives. If, in professionals' judgement, the evidence does not meet these criteria, they should obtain additional evidence or perform additional procedures to reduce the limitations or uncertainties related to the evidence. For example, a programme listing may not be adequate evidence until other evidence has been gathered to verify that it represents the actual programme used in the production process.

2.3.2 When evaluating reliability of evidence obtained during the audit, professionals should consider the characteristics and properties of the evidence, such as its source, nature (written, oral, visual or electronic), authenticity (presence of digital or manual signatures, date/time stamps), and relationships between evidence that provide corroborating evidence from multiple sources. In general, the reliability of evidence is ranked from low to high based on the procedures used to obtain the evidence as follows:

- Inquiry and confirmation
- Observation
- Inspection
- Analytical procedures
- Recalculation or computation
- Reperformance

For each of the previous procedures, evidence reliability is generally greater when it is:

- In written form, rather than obtained from oral representations
- Obtained directly by the professionals rather than indirectly by the entity being audited
- Obtained from independent sources
- Certified by an independent party
- Maintained by an independent party

2.3.3 Professionals should consider the period of time during which information exists or is available in determining the nature, timing and extent of substantive testing and, if applicable, compliance testing. For example, 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 the enterprise document retention policies.

2.3.4 If there is an independent third-party audit, professionals should consider whether testing of controls relevant to the subject of the audit was performed and whether any reliance can be placed on the results of that testing.

2.3.5 Professionals should obtain evidence that is sufficient and appropriate to enable a qualified independent party to reperform the tests and obtain the same results and conclusions.

2.4 Preparing Audit Documentation

2.4.1 During the performance of the audit, professionals should prepare documentation of the evidence obtained to be retained and available during a predefined time period and in a format that complies with enterprise policies and relevant professional standards, laws and regulations.

2.4.2 Evidence obtained during the performance of the audit should be appropriately identified, cross-referenced, and catalogued to facilitate determining the overall sufficiency and appropriateness of evidence to provide a reasonable basis for the findings and conclusions within the context of the audit objectives and to allow for easy retrieval by other IS audit team members or an independent party.

2.4.3 Professionals should ensure that documentation of evidence is protected from unauthorised access, disclosure or modification throughout its preparation and retention.

2.4.4 Professionals should dispose of evidence documentation at the end of the established retention period.

2205 Evidence *(cont.)*

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1203 Performance and Supervision	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. IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions.
1205 Evidence	IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. 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	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.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 process
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes*.

COBIT 5 Process	Process Purpose
MEA02 Monitor, evaluate and assess the system of internal controls.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
- Colleagues from within the enterprise
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations or professional media groups
- Other professional guidance (e.g., books, papers, other guidelines)

2205 Evidence *(cont.)*

4. Terminology

Term	Definition
Appropriate evidence	The measure of the quality of the evidence
Representation	A signed or oral statement issued by management to professionals, where management declares that a current or future fact (e.g., process, system, procedure, policy) is or will be in a certain state, to the best of management's knowledge
Sufficient evidence	The measure of the quantity of evidence; supports all material questions to the audit objective and scope. See evidence.

5. Effective Date

5.1 Effective Date This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2206 Using the Work of Other Experts

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 This guideline provides guidance to IS audit and assurance professionals when considering the use of work of other experts. The guideline assists in assessing the adequacy of the experts, reviewing and evaluating the work of other experts, assessing the need for performing additional test procedures and expressing an opinion for the audit engagement, while taking into account the work performed by other experts.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1007 Assertions
1.2.2 Standard 1203 Performance and Supervision
1.2.3 Standard 1206 Using the Work of Other Experts

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Considering the use of work of other experts
2.2 Assessing the adequacy of other experts
2.3 Planning and reviewing the work of other experts
2.4 Evaluating the work of other experts who are not part of the audit engagement team
2.5 Additional test procedures
2.6 Audit opinion or conclusion

2206 Using the Work of Other Experts *(cont.)*

2.1 Considering the Use of Work of Other Experts

2.1.1 When professionals do not have the required competencies to perform (part of) the audit engagement, they should consider seeking assistance from other experts with the required skills.

2.1.2 Using the work of other experts should be considered when there are constraints that could impair the audit work to be performed, e.g., technical knowledge required by the nature of the tasks to be performed, scarce audit resources, time constraints and to address potential independence issues. The use of other experts should also be considered if this results in a gain in the quality of the engagement.

2.1.3 Professionals should have sufficient knowledge of the work performed to guide and review the work, but should not be expected to have a knowledge level equivalent to the experts.

2.1.4 Professionals should base their choice of specific experts and the use of the other experts' work on objective criteria.

2.1.5 Professionals should communicate and document the performance requirements to other experts in a contract or agreement prior to the other experts beginning work on the engagement.

2.1.6 Where other expert's access to records or systems is prohibited by enterprise internal policies, professionals should determine the appropriate extent of the use and reliance on the other expert's work.

2.1.7 If the necessary experts cannot be obtained, professionals should document the impact on achieving the audit objectives and include specific tasks in the audit plan to manage the resulting audit risk. If the resulting audit risk cannot be managed, professionals may need to decline the audit engagement.

2.2 Assessing the Adequacy of Other Experts

2.2.1 When an audit engagement involves using the work of other experts, professionals should consider the adequacy of the other experts whilst planning the IS audit work. This includes:
- Assessing the independence and objectivity of the other experts
- Assessing their professional qualifications, competencies, relevant experience, resources and use of quality control processes

2.2.2 Professionals should consider carefully the independence and objectivity of other experts when using their work. The processes for selection and appointment, the organisational status, the reporting line and the effect of their recommendations on management practices are typical indicators of the independence and objectivity of other experts.

2.3 Planning and Reviewing the Work of Other Experts

2.3.1 Professionals should consider the activities of other experts and their effect on the IS audit objectives while planning the IS audit work. This includes:
- Obtaining an understanding of their scope of work, approach, timing and use of quality control processes
- Determining the level of review required

2.3.2 Professionals should verify that the audit charter or engagement letter specifies their right of access to the other experts' work. Professionals should have access to all work papers, supporting documentation and reports created by the other experts, where such access does not create legal issues.

2.3.3 The nature, timing and extent of audit evidence required will depend upon the significance and scope of the other experts' work. During the planning process, professionals should identify the level of review that is required to provide sufficient and appropriate audit evidence to achieve the overall IS audit objectives effectively. Professionals should review the other experts' final report, methodology or audit programme(s), and work papers.

2.3.4 In reviewing other experts' work papers, professionals should assess that the other experts' work was appropriately planned, supervised, documented and reviewed, to consider the appropriateness and sufficiency of the audit evidence provided by them, and to determine the extent of use and reliance on the expert's work. This assessment may include a retest of the work of other experts. Compliance with relevant professional standards should also be assessed. Overall, professionals should assess whether the work of other experts is adequate and complete to enable them to conclude on the current IS audit objectives and document a conclusion.

2.3.5 Professionals should perform sufficient reviews of the other experts' final report(s) to confirm that:
- The scope specified in the audit charter, terms of reference or letter of engagement has been met.
- Any significant assumptions used by the other experts have been identified.
- The findings and conclusions reported are adequately supported by evidence.

2206 Using the Work of Other Experts *(cont.)*

2.4 Evaluating the Work of Other Experts Who Are Not Part of the Audit Engagement Team

2.4.1 Today's interdependencies between customers and suppliers regarding the processing and outsourcing of non-core activities leads to a more complex audit environment. Parts of the environment being audited can be controlled and audited by other independent functions or organisations. As a result, the outsourcing organisation will receive reports from those third parties about the control environment of the outsourced operations. In some cases this may lessen the need for IS audit coverage even though professionals do not have access to supporting documentation and work papers. Professionals should be cautious in providing an opinion on such cases.

2.4.2 Professionals 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 professionals' responsibility to determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report. Professionals should also assess the effect of the other experts' findings and conclusions on the overall IS audit objective, and verify that any additional work required to meet the overall IS audit objective is completed. All assertions made by the other experts should be verified and formally approved by management; detailed guidance on this topic can be found in Standard 1007 Assertions.

2.5 Additional Test Procedures

2.5.1 Based on the assessment of the work of other experts, professionals should apply additional test procedures to gain sufficient and appropriate audit evidence in circumstances where the work of other experts does not provide such evidence.

2.5.2 Professionals should also consider whether supplemental testing of the other experts' work is required.

2.6 Audit Opinion or Conclusion

2.6.1 It remains professionals' ultimate responsibility to formulate an audit opinion or conclusion. Professionals need to determine if the work performed by other experts was sufficient to arrive to the audit opinion or conclusion.

2.6.2 If additional test procedures performed do not provide sufficient and appropriate audit evidence, professionals should provide an appropriate audit opinion or conclusion and include scope limitations where required.

2.6.3 Professionals' views and comments on the adoptability and relevance of the other experts' report should form a part of the audit engagement report if the experts' report is utilised in forming professionals' opinion.

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

---

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:

3.1 Linkage to standards

3.2 Linkage to COBIT 5 processes

3.3 Other guidance

2206 Using the Work of Other Experts *(cont.)*

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1007 Assertions	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.
1203 Performance and Supervision	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. 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.
1206 Using the Work of Other Experts	IS audit and assurance professionals shall consider using the work of other experts for the engagement, where appropriate. 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. 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. 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. 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. 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. 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.

2206 Using the Work of Other Experts *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 process
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
- Colleagues from within the enterprise
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations or professional media groups
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

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

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2207 Irregularity and Illegal Acts

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to provide IS audit and assurance professionals with guidance on how to deal with irregularities and illegal acts.

1.1.2 The guideline details the responsibilities of both management and IS audit and assurance professionals with regards to irregularities and illegal acts. It furthermore provides guidance on how to deal with irregularities and illegal acts during the planning and performance of the audit work. Finally, the guideline suggests good practices for internal and external reporting on irregularities and illegal acts.

1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standards, use professional judgement in their application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1005 Due Professional Care
1.2.2 Standard 1201 Engagement Planning
1.2.3 Standard 1202 Risk Assessment in Planning
1.2.4 Standard 1207 Irregularity and Illegal Acts
1.2.5 Standard 1401 Reporting

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Irregularities and illegal acts
2.2 Responsibilities of management
2.3 Responsibilities of the professionals
2.4 Irregularities and illegal acts during engagement planning
2.5 Designing and reviewing engagement procedures
2.6 Responding to irregularities and illegal acts
2.7 Internal reporting
2.8 External reporting

2207 Irregularity and Illegal Acts *(cont.)*

2.1 Irregularities and Illegal Acts

2.1.1 Irregularities and illegal acts can directly impact an enterprise in many (negative) ways, affecting finances and reputation, as well as indirectly affecting productivity and the retention of employees. Therefore, it is important that enterprises have awareness, prevention and detection mechanisms in place to identify irregularities and illegal acts quickly. Irregularities and illegal acts are more likely to occur in areas where there are non-existent, poorly designed or malfunctioning controls.

2.1.2 Irregularities and illegal acts can be committed by an employee at any level within the enterprise and may include activities such as, but not limited to:

- Fraud, which is any act involving the use of deception to obtain illegal advantage
- Deliberate misrepresentation of facts with the aim of gaining illegal advantage or hiding irregularities or illegal acts
- Acts that involve non-compliance with laws and regulations, including the failure of IT systems to meet applicable laws and regulations
- Unauthorised disclosure of data that is subject to privacy laws
- Acts that involve non-compliance with enterprise 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 (e.g., false disbursement, payroll fraud, tax evasion)
- Misappropriation and misuse of assets
- Skimming or defalcation, which is the misappropriation of cash before it is recorded in the financial records of an enterprise
- Acts, whether intentional or unintentional, that violate intellectual property (IP) rights, 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

2.1.3 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. Professionals 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.

2.1.4 Not all irregularities should be considered fraudulent activities. The determination of fraudulent activities depends on the legal definition of fraud in the respective jurisdiction. Fraudulent 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
- 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 enterprise as a whole
- Gross negligence
- Unintentional illegal acts

2207 Irregularity and Illegal Acts *(cont.)*

2.2 Responsibilities of Management

2.2.1 It is primarily management's and the board's responsibility to provide controls to deter, prevent and detect irregularities and illegal acts.

2.2.2 Management typically uses the following means to obtain reasonable assurance that irregularities and illegal acts are deterred, 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.
- Policies 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
- Policies and procedures governing compliance and regulatory requirements

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

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

2.3 Responsibilities of the Professionals

2.3.1 Professionals should consider defining in the audit charter the responsibilities of management and IS audit and assurance management 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 enterprise policy or a similar document, the audit charter should include a statement to that effect.

2.3.2 Professionals should understand that control mechanisms cannot completely eliminate the possibility of irregularities or illegal acts occurring. Professionals are 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.

2.3.3 Professionals are not responsible for the prevention or detection of irregularities or illegal acts. An audit engagement cannot guarantee that irregularities will be detected. Even when an audit is planned and performed appropriately, irregularities could go undetected, e.g., if there is collusion between employees, collusion between employees and outsiders, or management involvement in the irregularities. The aim is to determine the control is in place, adequate, effective and complied with.

2.3.4 Where professionals have specific information about the existence of an irregularity or illegal act, they have an obligation to report it.

2.3.5 Professionals should inform management and those charged with governance when they have identified situations where a higher level of risk exists for a potential irregularity or illegal act, even if none is detected.

2.3.6 Professionals should be reasonably familiar with the area under review to be able to identify risk factors that may contribute to the occurrence of irregular or illegal acts.

2.4 Irregularities and Illegal Acts During Engagement Planning

2.4.1 Professionals 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, professionals 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, enterprise direction
- The history of the enterprise, 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 current strategic direction of the enterprise
- 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

2207 Irregularity and Illegal Acts *(cont.)*

2.4 Irregularities and Illegal Acts During Engagement Planning (cont.)

- 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
- Audit findings from previous audits
- The industry and competitive environment in which the enterprise operates
- Findings of reviews conducted 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
- Existence of process documentation and/or 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 for core business systems compared with packaged software
- 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

2.4.2 As part of the planning process and performance of the risk assessment, professionals should inquire of management, and obtain written representations if appropriate, 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
- Management responsibility for designing and implementing internal controls to prevent irregularities and illegal acts
- How the risk of irregularities or illegal acts is monitored or managed
- What processes are in place to communicate about alleged, suspected or existent irregularities or illegal acts to appropriate stakeholders
- Applicable national and regional laws in the jurisdiction in which the organisation operates and the extent of coordination the legal department has with the risk committee and/or audit committee

2.5 Designing and Reviewing Engagement Procedures

2.5.1 While professionals have no explicit responsibility to detect or prevent illegal acts or irregularities, they should design procedures for the audit engagement that take into account the level of risk for irregularities and illegal acts that has been identified.

2.5.2 Professionals 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 the following are identified:

- Irregularities that could have a material effect on the area under audit, or on the enterprise as a whole
- Control weaknesses that would fail to prevent or detect material irregularities
- 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

2.5.3 Professionals should review the results of engagement procedures to determine whether there are indications that irregularities or illegal acts may have occurred. Using computer assisted audit techniques (CAATs) could aid significantly in the effective and efficient detection of irregularities or illegal acts.

2.5.4 When this evaluation is performed, risk factors identified in 2.4.1 should be reviewed against the actual procedures performed to provide reasonable assurance that all identified risk has been addressed.

2207 Irregularity and Illegal Acts *(cont.)*

2.6 Responding to Irregularities and Illegal Acts

2.6.1 During an audit engagement, indications of the existence of irregularities or illegal acts may come to the attention of professionals. They should consider the potential effect of the irregularities or illegal acts on the subject matter of the engagement, the audit objectives, the audit engagement report and the enterprise.

2.6.2 Professionals should demonstrate an attitude of professional scepticism. Indicators (sometimes called 'Fraud or Red Flags') of persons committing irregularities or illegal acts are:

- Overrides of controls by management
- Irregular or poorly explained management behaviour
- Consistently over performing, compared to set targets
- Problems with, or delays in, receiving requested information or evidence
- Transactions not following the normal approval cycles
- Increase in activity of a certain customer
- Increase in complaints from customers
- Deviating access controls for some applications or users

Professionals should pay close attention when noticing these behaviours.

2.6.3 When professionals become aware of information concerning a possible irregularity or illegal act, they should consider taking the following steps after direction from the appropriate legal authority:

- Obtain an understanding of the nature of the act
- Understand the circumstances in which the act occurred
- Gather evidence of the occurrence of the act (e.g., letters, system records, computer files, security logs, customer of vendor information)
- Identify all persons involved in committing the act
- Obtain sufficient supportive information to evaluate the effect of the act
- Perform limited additional procedures to determine the effect of the act and whether additional acts exist
- Document and preserve all evidence and work performed

2.6.4 Professionals should then consult with audit management to determine their next actions which may involve reporting the 'event' to enterprise management, passing further action to internal fraud investigators, and/or reporting to law enforcement or regulators.

2.6.5 When an irregularity involves a member of management, professionals should reconsider the reliability of representations made by management. Typically, professionals should work with an appropriate level of management above the one associated with the irregularity or illegal act.

2.7 Internal Reporting

2.7.1 The detection of irregularities and illegal acts should be communicated (in writing or orally) to the appropriate people in the enterprise in a timely manner by professionals. The notification should be directed to a level of management above that at which the irregularities and illegal acts are suspected to have occurred. In addition, irregularities and illegal acts should be reported to those charged with governance in the enterprise, such as the board of directors, trustees, audit committee or equivalent body, except for matters that are clearly insignificant in terms of both financial effect and indications of control weaknesses.

If professionals suspect that all levels of management are involved, then the findings should be confidentially reported directly to those charged with enterprise governance, such as the board of directors, trustees, audit committee or equivalent body, according to the local applicable laws and regulations. Local laws and regulations may prohibit reporting to parties other than the prescribed legal authority.

2.7.2 Professionals should use professional judgement when reporting an irregularity or illegal act. They 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 professionals maintain their independence.

2207 Irregularity and Illegal Acts *(cont.)*

2.7 Internal Reporting (cont.)

2.7.3 The individuals included in the internal distribution of reports of irregularities or illegal acts should be considered carefully. The occurrence and effect of irregularities or illegal acts is a sensitive issue and report distribution carries its own risk, 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 enterprise
- Loss of key staff and management, including those not involved in the irregularity or illegal act, because confidence in management and the future of the enterprise decreases

2.7.4 Professionals should consider reporting the irregularity or illegal act separately from any other audit issues if this would assist in controlling the distribution of the report.

2.7.5 Professionals 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.

2.7.6 The audit charter should define professionals' responsibilities with regards to reporting irregularities or illegal acts.

2.8 External Reporting

2.8.1 External reporting of fraud, irregularity or illegal acts may be a legal or regulatory obligation. The obligation may apply to enterprise management or the individuals involved in detecting the irregularities, or both. Legal reporting requirements for the auditor are subject to local jurisdiction and supercede internal policy and/or contractual agreements. Additional situations that may require external reporting include:
- Compliance with legal or regulatory requirements
- Court order
- Funding agency or government agency in accordance with requirements for the audits of entities that receive governmental financial assistance
- External auditor requests

2.8.2 Where external reporting is required, prior to external release the form and content of the information reported should be approved by the appropriate level of IS audit and assurance management and reviewed with auditee executive management, unless prevented by applicable regulations or specific circumstances of the audit engagement. Examples of specific circumstances that may prevent obtaining auditee executive management's agreement include:
- Auditee executive management's active involvement in the irregularity or illegal act
- Auditee executive management's passive acquiescence to the irregularity or illegal act

2.8.3 If auditee executive management does not agree to the external release of the report, and external reporting is a statutory or a regulatory obligation, then professionals should consider consulting the audit committee and legal counsel about the advisability and risk of reporting the findings outside the enterprise. Even in situations where professionals are protected by privilege, they should seek legal advice and counsel prior to making this type of disclosure to ensure that they are in fact protected by this privilege.

2.8.4 Professionals, with the approval of IS audit and assurance management, should report irregularities or illegal acts to appropriate regulators on a timely basis. If the enterprise fails to disclose a known irregularity or illegal act or requires professionals to suppress these findings, professionals should seek legal advice and counsel.

2.8.5 If an irregularity or illegal act has been detected by professionals, then they should inform the external auditors in a timely manner.

2.8.6 Where professionals are aware that management is required to report fraudulent activities to an outside organisation, the professionals should formally advise management of this responsibility.

2207 Irregularity and Illegal Acts *(cont.)*

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA Standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1005 Due Professional Care	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.
1201 Engagement Planning	IS audit and assurance professionals shall plan each IS audit and 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
1202 Risk Assessment in Planning	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. IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements. IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.
1207 Irregularity and Illegal Acts	IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement. IS audit and assurance professionals shall maintain an attitude of professional scepticism during the engagement. IS audit and assurance professionals shall document and communicate any material irregularities or illegal act to the appropriate party in a timely manner.
1401 Reporting	IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient, reliable and relevant evidence.

2207 Irregularity and Illegal Acts *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:

- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM03 Ensure risk optimisation.	Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
APO12 Manage risk.	Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:

- Colleagues from within the enterprise
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

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.
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

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2208 Sampling

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to provide guidance to IS audit and assurance professionals to design and select an audit sample and evaluate sample results. Appropriate sampling and evaluation will help in achieving the requirements of sufficient and appropriate evidence.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement related standards, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1006 Proficiency
1.2.2 Standard 1202 Risk Assessment in Planning
1.2.3 Standard 1203 Performance and Supervision
1.2.4 Standard 1205 Evidence

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Sampling
2.2 Design of the sample
2.3 Selection of the sample
2.4 Evaluation of sample results
2.5 Documentation

2.1 Sampling

2.1.1 In forming an opinion or conclusion, professionals frequently do not examine all of the information available as it may be impractical (e.g., requiring too much time for both the auditee as well as professionals to investigate all information) and valid conclusions can be reached using audit sampling.

2.1.2 When using either statistical or non-statistical sampling methods, the professionals should design and select an audit sample, perform audit procedures and evaluate sample results to obtain sufficient and appropriate evidence to form a conclusion. When using sampling methods to draw a conclusion on the entire population, professionals should use statistical sampling.

2208 Sampling *(cont.)*

2.2 Design of the Sample

2.2.1 When designing the size and structure of an audit sample, professionals should consider the specific IS audit objectives, the audit procedures that are most likely to achieve those objectives, the nature of the population, relevant subgroups within the population, and the sampling and selection methods. In addition, when audit sampling is appropriate, consideration should be given to the nature of the evidence sought, possible error conditions and possible root causes.

2.2.2 When designing the audit sample, while taking into account the IS audit objectives professionals should consider:
- Purpose of the sample
- Sampling unit
- Population
- Sampling risk and sample size
- Tolerable error
- Underlying expected distribution (e.g., Poisson, binomial, normal, exponential)
- Behaviour over time (e.g., seasonality, decrement in performance)
- Subpopulations or subgroups that are naturally occurring and should be considered for operational relevance
- Outliers
- Small populations of adverse or rare events
- Data from external support tools, used to confirm or complement the results of sampling

2.2.3 Professionals should consider the purpose of the sample:
- **Compliance testing/test of controls**—An audit procedure designed to evaluate the operating effectiveness of controls in preventing or detecting and correcting material weaknesses. Examples of compliance testing of controls, where sampling could be considered, include user access rights, program change control procedures, procedure documentation, program documentation, follow-up on exceptions, review of logs and software licences audits.
- **Substantive testing/test of details**—An audit procedure designed to detect material weaknesses at the assertion level. Examples of substantive tests, where sampling could be considered, include reperformance of a complex calculation (e.g., interest) on a sample of accounts, a sample of transactions to vouch to supporting documentation, etc.

2.2.4 The sampling unit depends on the purpose of the sample. For compliance testing of controls, where the sampling unit is an event or transaction (e.g., a control such as authorisation of an invoice), attribute sampling is typically applied as it is used to determine the characteristics of a population. For substantive testing, where the sampling unit is often monetary, variables sampling is frequently applied because it is used to determine the monetary or volumetric impact of characteristics of a population.

2.2.5 The population is the entire set of data from which professionals wish to sample to reach a conclusion on the population. Therefore, the population from which the sample is drawn has to be appropriate to test the design and/or operating effectiveness of the controls, and verified as complete for the specific IS audit objective and scope.

2.2.6 To assist in the efficient and effective design of the sample, sampling 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, professionals should consider the sampling risk, the amount of the error that would be acceptable and the extent to which errors are expected. Sampling risk arises from the possibility that professionals' 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**—A material weakness is assessed as unlikely when, in fact, the population is materially misstated.
- **The risk of incorrect rejection**—A material weakness is assessed as likely when, in fact, the population is not materially misstated.

2.2.8 Sample size is affected by the level of sampling risk that the professionals are 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, as detailed in Standard 2202 Risk Assessment in Planning.

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

2208 Sampling *(cont.)*

2.2 Design of the Sample (cont.)

2.2.10 If professionals expect errors to be present in the population, a larger sample than when no error is expected has to be examined to conclude that the actual error in the population is not greater than the expected tolerable error. Smaller sample sizes are justified when the population is expected to be error free. When estimating the expected error in a population, professionals should consider such matters as:
- Error levels identified in previous audits
- Changes in enterprise procedures
- Evidence available from an evaluation of the system of internal control, results from analytical review procedures, and/or results of preliminary tests of the population

2.2.11 Professionals should consider, if appropriate, the need to involve specialists in the design and analysis of complex sampling approaches, such as stratified random samples that must have statistical validity, or sampling based in established quality control methods (e.g., Six Sigma).

2.2.12 Should professionals conclude that sampling does not allow achieving the IS audit objectives and a test of the entire population is required, they should consider applying continuous assurance because it allows testing of the entire population in a timely and cost-effective way.

2.3 Selection of the Sample

2.3.1 Professionals should ensure that the population is complete and control the selection of the sample, to maintain audit independence. Professionals should select sample items in such a way that the sample is expected to be representative of the population regarding the characteristics being tested.

2.3.2 For a sample to be representative of the entire population, all sampling units in the population should have an equal or known, non-zero probability of being selected. This implies using statistical sampling methods, because they involve the use of techniques from which mathematically constructed conclusions regarding the entire population can be drawn. Professionals should thus validate completeness of the population to ensure that the sample is selected from an appropriate data set.

2.3.3 Non-statistical sampling is an approach used by professionals who want to use their own experience, knowledge and professional judgement to determine a sample. This method implies a human bias because it is not statistically based, does not ensure that every sampling unit has a known, non-zero probability of being selected, and thus results should not be extrapolated over the population because the sample is unlikely to be representative of the entire population. Non-statistical sampling may be used when results are needed quickly to confirm a proposition and should not be used to draw mathematically constructed conclusions regarding the entire population.

2.3.4 There are five commonly used sampling methods, divided into either statistical sampling methods or non-statistical sampling methods:
- Statistical sampling methods are:
  - **Simple 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., $1000) in the population is given an equal chance of selection. Because ordinarily the individual monetary unit cannot be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weighs the selection in favour of the larger amounts. Another example includes selecting every 'nth' sampling unit.
  - **Stratified random sampling**—Ensures that all sampling units in each subgroup have a known, non-zero chance of selection.

  Professionals should consider using statistical software for calculating standard deviations and other summary statistics for results of statistical sampling.
- Non-statistical sampling methods are:
  - **Haphazard sampling**—Professionals select 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.
  - **Judgemental sampling**—Professionals place a bias on the sample (e.g., all sampling units over a certain value, all for a specific type of exception, all negatives). It should be noted that a judgemental sample is not statistically based and results should not be extrapolated over the population because the sample is unlikely to be representative of the population as a whole.

2208 Sampling *(cont.)*

2.3 Selection of the Sample (cont.)

2.3.5 There are two commonly used selection methods:

- Selection on records and population subgroups; common methods are:
  - Simple random sampling
  - Stratified random sampling
  - Haphazard sampling
  - Judgemental sample
- Selection on quantitative fields (e.g., monetary units); common methods are:
  - Simple random sampling
  - Systematic sampling

2.4 Evaluation of Sample Results

2.4.1 Having performed those audit procedures that are appropriate to the particular IS audit objective on each sample item, professionals 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 actual errors, the errors should be projected as appropriate to the population, but only if the sampling method used is statistically based.

2.4.2 Any possible errors detected in the sample should be reviewed to determine whether they are actually errors. Professionals 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. For example, errors that are the result of the breakdown of an automated process normally have wider implications than human errors.

2.4.3 When the expected audit evidence regarding a specific sample unit cannot be obtained, professionals should consider whether they are able to obtain sufficient and appropriate audit evidence by performing alternative procedures on the item selected, or by selecting and testing a replacement sample unit.

2.4.4 Professionals 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.

2.4.5 Discussion of the results of non-statistical sampling (haphazard or judgmental) should be restricted to a description of the results of analyzing the sample, in context of the population as a whole.

2.4.6 Professionals should consider whether errors in the population might exceed the tolerable error by comparing the projected population error to the estimated or defined tolerable error, taking into account the results of other audit procedures relevant to the audit objective. Tolerable error may be estimated or defined by audit criteria, industry standards, contractual requirements, software specifications, etc. When the projected population error exceeds the tolerable error, professionals should reassess the sampling risk and, if that risk is unacceptable, consider extending the audit procedure, recalculating sample size using the refined tolerable error and testing the additional sample units, or performing alternative audit procedures.

2.5 Documentation

2.5.1 The work papers should include sufficient detail to describe clearly the sampling objective and the sampling process used. The work papers should include:

- Purpose of the sample, including sample unit
- Source of the population, definition of the population, and its relation to the audit scope
- Sampling parameters, e.g., sample size (including any consideration with regards to sampling risk), random start or seed number or method by which random start was obtained, sampling interval
- Sampling method
- Items selected and, if non-statistical sampling is used, justification for the selected items
- Details of audit tests performed, including evaluation of errors and, if applicable, alternative audit procedures
- Conclusions reached

2208 Sampling *(cont.)*

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1006 Proficiency	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.
1202 Risk Assessment in Planning	IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.
1203 Performance and Supervision	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. IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions. IS audit and assurance professionals shall identify and conclude on findings.
1205 Evidence	IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
APO12 Manage risk.	Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

2208 Sampling *(cont.)*

3.3 Other Guidance When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:

- Colleagues from within the enterprise
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Attribute sampling	Method to select a portion of a population based on the presence or absence of a certain characteristic
Audit sampling	The application of audit procedures to less than 100 percent of the items within a population to obtain audit evidence about a particular characteristic of the population
Non-statistical sampling	Method of selecting a portion of a population, by means of own judgement and experience, for the purpose of quickly confirming a proposition. This method does not allow drawing mathematical conclusions on the entire population.
Population	The entire set of data from which a sample is selected and about which an IS auditor wishes to draw conclusions.
Sampling risk	The probability that an IS auditor has reached an incorrect conclusion because an audit sample, rather than the entire population, was tested. Scope Notes: While sampling risk can be reduced to an acceptably low level by using an appropriate sample size and selection method, it can never be eliminated.
Sampling stratification	The process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum
Statistical sampling	A method of selecting a portion of a population, by means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population.
Tolerable error	The maximum error in the population that professionals are willing to accept and still conclude that the test objective has been achieved. For substantive tests, tolerable error is related to professionals' judgement about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the professionals are willing to accept.
Variable sampling	A sampling technique used to estimate the average or total value of a population based on a sample; a statistical model used to project a quantitative characteristic, such as a monetary amount

5. Effective Date and Review Date

5.1 Effective Date This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

Reporting Guidelines

The reporting guidelines are:
2401 Reporting
2402 Follow-up Activities

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

2401 Reporting

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 This guideline provides guidance for IS audit and assurance professionals on the different types of IS audit engagements and related reports.

1.1.2 The guideline details all aspects that should be included in an audit engagement report and provides IS audit and assurance professionals with considerations to make when drafting and finalising an audit engagement report.

1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1007 Assertions
1.2.2 Standard 1205 Evidence
1.2.3 Standard 1401 Reporting
1.2.4 Standard 1402 Follow-up Activities

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Types of engagements
2.2 Required contents of the audit engagement report
2.3 Subsequent events
2.4 Additional communication

2401 Reporting *(cont.)*

2.1 Types of Engagements

2.1.1 Professionals may perform any of the following types of audit engagements:
- Examination
- Review
- Agreed-upon procedures

Note: These terms are defined in ITAF, 2nd Edition.

2.1.2 Both examination and review engagements 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 both types of engagements)
- Forming a conclusion about, and reporting on, the design and/or operating effectiveness of the control procedures based on the identified criteria:
  – The conclusion for a reasonable assurance engagement is expressed as a positive opinion and provides a high level of assurance.
  – The conclusion for a limited assurance engagement is expressed as a negative opinion and provides only a moderate level of assurance.

2.1.3 An 'agreed-upon procedures' engagement does not result in the expression of any assurance by professionals. Professionals are engaged to carry out specific procedures to meet the information needs of those parties who have agreed to the procedures to be performed (e.g., executive management, the board or those charged with governance). Professionals issue 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 nature, timing and extent of procedures do not enable the professional to express any assurance. The report is restricted to those parties that have agreed to the procedures to be performed because others are not aware of the reasons for the procedures and may misinterpret the result.

2.1.4 An agreed-upon procedures report could also be distributed to a third party (e.g., regulatory body) when predetermined and approved by the parties that have agreed on the procedures before the start of the actual work. Professionals should consider this, using their professional judgement, based on the risk of misinterpretation of the work to be performed.

2.1.5 Professionals, who before the completion of an audit engagement are requested to change the audit engagement from an examination or review engagement to an agreed-upon procedures engagement, need 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 qualified report.

2401 Reporting *(cont.)*

2.2 Required Contents of the Audit Engagement Report

2.2.1 In developing an audit engagement 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. Professionals should conclude whether sufficient and appropriate evidence has been obtained to support the conclusions in the audit engagement report. More detailed guidance can be found in Standard 1205 Evidence.

2.2.2 When concluding on an examination or review engagement, professionals should come to an expression of opinion about whether, in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective. This opinion can be:

- **Unqualified**—Professionals should express an unqualified opinion when they conclude that, in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective, in accordance with the applicable criteria.
- **Qualified**—Professionals should express a qualified opinion when they:
  - Having obtained sufficient and appropriate evidence, conclude that control weaknesses, individually or in the aggregate, are material, but not pervasive to the IS audit objectives
  - Are unable to obtain sufficient and appropriate evidence on which to base the opinion, but conclude that the possible effects on the IS audit objectives of undetected weaknesses, if any, could be material but not pervasive
- **Adverse**— Professionals should express an adverseopinion when one or more significant deficiencies aggregate to a material and pervasive weakness
- **Disclaimer**—Professionals should disclaim an opinion when they are unable to obtain sufficient and appropriate evidence on which to base the opinion, and conclude that the possible effects on the IS audit objectives of undetected weaknesses, if any, could be both material and pervasive.

2.2.3 Professionals' examination or review report about the effectiveness of control procedures should include the following elements:

- An appropriate and distinctive title, clearly distinguishing the report from any other type of report not subject to auditing standards
- Identification of the recipients to whom the report is directed, according to the terms in the audit charter or engagement letter
- Identification of the responsible party, including a statement of the party responsible for the subject matter
- Description of the scope of the audit engagement, 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 professionals' 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
- A statement identifying the source of management's representation about the effectiveness of control procedures
- A statement that professionals have conducted the audit engagement to express an opinion on the effectiveness of control procedures
- Identification of the purpose (i.e., IS audit objectives) for which professionals' 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. Furthermore, the professionals should consider disclosing:
  - Any significant interpretations made in applying the criteria
  - Measurement methods used when criteria allow for a choice between a number of measurement methods
  - Changes in the standard measurement methods used

2401 Reporting *(cont.)*

2.2 Required Contents of the Audit Engagement Report (cont.)

- Statement that the audit engagement has been conducted in accordance with ISACA IS audit and assurance standards or other applicable professional standards. Any non-compliance with these standards should be explicitly mentioned in the report.
- Further explanatory details about the variables that affect the assurance provided and other information as appropriate
- Findings, conclusions and recommendations for corrective action and include management's response. For each management response, professionals should obtain information on the proposed actions to implement or address reported recommendations and the planned implementation or action date.
  - Responsible management may decide to accept the risk of not correcting a reported condition because of cost, complexity of the corrective action or other considerations. The board of directors (or those charged with governance) should be informed of recommendations for which management accepts the risk of not correcting the reported situation.
  - If professionals and the auditee disagree about a particular recommendation or audit comment, the engagement communications may state both positions and the reasons for the disagreement. The auditee's written comments may be included as an appendix to the engagement report. Alternatively, the auditee's views may be presented in the body of the report or in a cover letter. Executive management, or those charged with governance, should then make a decision as to which point of view they support.
- 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 engagement is not designed to detect all weaknesses in control procedures because it is not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis.
- A summary of the work performed, which will help the intended users of the report to better understand the nature of the assurance conveyed
- An expression of opinion about whether, in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective. When professionals' opinion is qualified, a paragraph describing the reasons for qualification should be included.
- Where appropriate, references to any other separate reports that should be considered, such as a separate report that communicates security vulnerabilities that are protected from disclosure and should be distributed to a restricted list of recipients
- Date of issuance of the audit engagement report. In most instances, the date of the report is based upon the issue date. It is recommended to also mention the dates when the audit work was actually performed, if not yet mentioned with the summary of the work performed.
- Names of individuals or entity responsible for the report, appropriate signatures and locations

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

- An appropriate and distinctive title, clearly distinguishing the report from any other type of report not subject to auditing standards
- Identification of the recipients to whom the report is directed, according to the terms in the audit charter
- Identification of the responsible party, including a statement of the party responsible for the subject matter
- A statement that the audit engagement has been conducted in accordance with ISACA IS audit and assurance standards or other applicable professional standards. Any non-compliance with these standards should be explicitly mentioned in the report.
- Identification of the subject matter (or the written assertion related thereto) and the purpose (i.e., IS audit objectives) of the audit engagement
- A statement that the procedures performed were those agreed to by the responsible parties identified in the report
- A statement that the sufficiency of the procedures is solely the responsibility of the responsible parties and a disclaimer of responsibility for the sufficiency of those procedures

2401 Reporting *(cont.)*

2.2 Required Contents of the Audit Engagement Report (cont.)

- A list of the procedures performed (or reference thereto)
- A description of the findings, including sufficient details of errors and exceptions found
- A statement that professionals only performed the agreed-upon procedures and, as such, no assurance is expressed
- A statement that if the professionals had performed additional procedures, other matters might have come to professionals' 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
- A statement that the report only relates to the elements specified and that it does not extend beyond them
- References to any other separate reports that should be considered
- Date of issuance of the audit engagement report. In most instances, the date of the report is based upon the issue date. It is recommended to also mention the dates when the audit work was actually performed, if not yet mentioned with the summary of the work performed.
- Names of individuals or entity responsible for the report, appropriate signatures and locations

2.2.5 There are two types of examination reports:

- **Direct reports**—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.
- **Indirect reports**—Based on management assertions about the subject matter.

More detailed guidance on the difference between indirect and direct reporting can be found in Standard 1007 Assertions.

2.3 Subsequent Events

2.3.1 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 professionals' report, which have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject matter or assertions. These occurrences are referred to as subsequent events. In performing an audit engagement, professionals should consider information about subsequent events that comes to their attention. However, professionals have no responsibility to detect subsequent events.

2.3.2 Professionals should inquire with management as to whether they are aware of any subsequent events, through to the date of professionals' report, that would have a material effect on the subject matter or assertions.

2.4 Additional Communication

2.4.1 Professionals should 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.

2.4.2 Professionals should communicate significant deficiencies and material weaknesses in the control environment to those charged with governance and, where applicable, to the responsible authority. They should also explicitly disclose in the report that these have been communicated.

2.4.3 Professionals should communicate to 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 by the professionals that such internal control deficiencies have been communicated to management.

2.4.4 Professionals should obtain written representations from management acknowledging, at a minimum, the following assertions:

- Management responsibility for establishing and maintaining proper and effective internal controls, including systems of internal accounting and administrative controls over operating activities and information systems under review, and activities to identify all laws, rules and regulations, which govern the subject area under review, and to ensure compliance with them.
- All requested information relevant to the engagement objectives was provided to the engagement team including, but not limited to:
  - Records, related data, electronic files and reports
  - Policies and procedures
  - Pertinent personnel
  - Results of relevant internal and external IS audits, reviews and assessments

2401 Reporting *(cont.)*

2.4 Additional Communication (cont.)

- No event(s) has occurred or matters discovered since the end of fieldwork that would have a material effect on the engagement.
- Management has no knowledge of any fraud or suspected fraud, irregularities and illegal acts related to the subject area under review, including management and employees with responsibility for internal control not already disclosed.
- Management has no knowledge of any allegations of fraud or suspected fraud, irregularities and illegal acts affecting the area under review received in communications from employees, clients, contractors or others not already disclosed.
- Acknowledgement of responsibility for the design and implementation of programs and controls to prevent and detect fraud, irregularities and illegal acts.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1007 Assertions	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.
1205 Evidence	IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives
1401 Reporting	IS audit and assurance professionals shall provide a report to communicate the results upon completion of 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 IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient, reliable and relevant evidence.
1402 Follow Up	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.

2401 Reporting *(cont.)*

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM05 Ensure stakeholder transparency.	Make sure that the communication to stakeholders is effective and timely, and the basis for reporting is established to increase performance, identify areas for improvement and confirm that IT-related objectives and strategies are in line with the enterprise's strategy.
MEA01 Monitor, evaluate and assess performance and conformance.	Provide transparency of performance and conformance and drive achievement of goals.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
- Colleagues from within the enterprise
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Appropriate evidence	The measure of the quality of the evidence
Inconsequential deficiency	A deficiency is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected deficiencies, that the deficiencies, either individually or when aggregated with other deficiencies, would clearly be trivial to the subject matter. If a reasonable person could not reach such a conclusion regarding a particular deficiency, that deficiency is more than inconsequential.
Sufficient evidence	The measure of the quantity of evidence; supports all material questions to the audit objective and scope. See evidence.

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

2402 Follow-up Activities

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to provide guidance to IS audit and assurance professionals in monitoring if management has taken appropriate and timely action on reported recommendations and audit findings.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1401 Reporting
1.2.2 Standard 1402 Follow-up Activities

1.3 Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Follow-up process
2.2 Management's proposed actions
2.3 Assuming the risk of not taking corrective action
2.4 Follow-up procedures
2.5 Timing and scheduling of follow-up activities
2.6 Nature and extent of follow-up activities
2.7 Deferring follow-up activities
2.8 Form of follow-up responses
2.9 Follow-up by professionals on external audit recommendations
2.10 Reporting of follow-up activities

2402 Follow-up Activities *(cont.)*

2.1 Follow-up Process

2.1.1 Follow-up activity performed by professionals is a process by which they determine the adequacy, effectiveness and timeliness of actions taken by management on reported observations and recommendations, including those made by external auditors and others.

2.1.2 A follow-up process should be established to help provide reasonable assurance that each review conducted by professionals provides optimal benefit to the enterprise by requiring that agreed-on outcomes arising from reviews are implemented in accordance with management undertakings or that (executive) management recognises and acknowledges the risk of delaying or not implementing proposed outcomes and/or recommendations.

2.2 Management's Proposed Actions

2.2.1 As part of their discussions with the auditee, professionals should obtain agreement on the results of the audit engagement and on a plan of action to improve operations, as needed.

2.2.2 Professionals should discuss with management the proposed actions to implement or address reported recommendations and audit comments. These proposed actions should be provided to professionals and should be recorded as a management response in the final report with a committed implementation and/or action date.

2.2.3 If professionals and the auditee come to an agreement on the proposed actions, professionals should initiate the procedures for follow-up activities, as detailed in section 2.4.

2.3 Assuming the Risk of Not Taking Corrective Action

2.3.1 (Executive) management may decide to accept the risk of not correcting the reported condition because of cost, complexity of the corrective action or other considerations. The board (or those charged with governance) should be informed of (executive) management's decision on all significant engagement observations and recommendations for which management accepts the risk of not correcting the reported situation.

2.3.2 When professionals believe that the auditee has accepted a level of residual risk that is inappropriate for the enterprise, they should discuss the matter with IS audit and assurance management and executive management. If professionals remain in disagreement with the decision regarding residual risk, they, along with executive management, should report the matter to the board (or those charged with governance) for resolution.

2.3.3 Acceptance of risk should be documented and formally approved by executive management and communicated to those charged with governance.

2.4 Follow-up Procedures

2.4.1 Procedures for follow-up activities should be established and should include:
- The recording of a time frame within which management should respond to agreed-on recommendations
- An evaluation of management's response
- A verification of the response, if appropriate (refer to section 2.6)
- Follow-up work, if appropriate
- A communication procedure that escalates outstanding and unsatisfactory responses and/or actions to the appropriate levels of management and to those charged with governance
- A process for obtaining management's assumption of associated risk, in the event that corrective action is delayed or not proposed to be implemented

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

2.4.3 Factors that should be considered in determining appropriate follow-up procedures are:
- The importance and impact of the findings and recommendations
- Any changes in the IS environment that may affect the importance and impact of the findings and recommendations
- The complexity of correcting the reported situation
- The time, cost and effort needed to correct the reported situation
- The effect if correcting the reported situation should fail

2.4.4 Responsibility for follow-up actions, reporting and escalation should be defined in the audit charter.

2402 Follow-up Activities *(cont.)*

2.5 Timing and Scheduling of Follow-up Activities

2.5.1 The timing of the follow-up activities should take into account the significance of the reported findings and the effect if corrective actions are not taken. The timing of 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 risk and costs to the enterprise.

2.5.2 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 degree of difficulty, the risk and exposure involved, the results of the review, the time needed for implementing corrective actions, etc., and may be established in consultation with management.

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

2.5.4 The implementation of all the management responses may be followed up on a regular basis (e.g., each quarter) for different audit engagements 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 on with management.

2.6 Nature and Extent of Follow-up Activities

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

2.6.2 Management's response detailing the actions taken should be evaluated, if possible, by professionals who performed the original review. Wherever possible, audit evidence of action taken should be obtained.

2.6.3 Where management provides information on actions taken to implement recommendations and professionals have 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 further follow-up activities.

2.6.4 As a part of the follow-up activities, professionals should evaluate whether unimplemented recommendations are still relevant or have a greater significance. Professionals 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.

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

2.6.6 Professionals' opinion on unsatisfactory management responses or action should be communicated to the appropriate level of management.

2.7 Deferring Follow-up Activities

2.7.1 Professionals are 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 time needed in implementing corrective actions.

2.7.2 There may also be instances where professionals judge 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.

2402 Follow-up Activities *(cont.)*

2.8 Form of Follow-up Responses

2.8.1 The most effective way to receive follow-up responses from management is in writing, because 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 professionals and, where possible, approved by management. Proof of action or implementation of recommendations may also be provided with the response.

2.8.2 Professionals should request and/or receive periodic updates from management responsible for implementing agreed-on actions to evaluate the progress management has made, particularly in relation to high-risk issues and corrective actions with long lead times.

2.9 Follow-up by Professionals on External Audit Recommendations

2.9.1 Depending on the scope and terms of the audit engagement and in accordance with the relevant IS auditing standards, external professionals may rely on internal professionals to follow-up on their agreed-on recommendations. Responsibilities regarding this follow-up can be determined in the audit charter or engagement letters.

2.10 Reporting of Follow-up Activities

2.10.1 A report on the status of agreed-on corrective actions arising from audit engagement reports, including agreed-on recommendations not implemented, should be presented to the appropriate level of management and to those charged with governance (e.g., the audit committee).

2.10.2 If, during a subsequent audit engagement, professionals find that the corrective action that management had reported as 'implemented' had in fact not been implemented, they should communicate this to the appropriate level of management and those charged with governance. If appropriate, the professional should obtain a current corrective action plan and planned implementation date.

2.10.3 When all the agreed-on corrective actions have been implemented, a report detailing all the implemented and/or completed actions can be forwarded to executive management and those charged with governance.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

2402 Follow-up Activities *(cont.)*

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1401 Reporting	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 IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient, reliable and relevant evidence.
1402 Follow-up Activities	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.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose.

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes.*

COBIT 5 Process	Process Purpose
EDM01 Ensure governance framework setting and maintenance.	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.
EDM02 Ensure benefits delivery.	Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
EDM03 Ensure risk optimisation.	Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

2402 Follow-up Activities *(cont.)*

3.3 Other Guidance When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:

- Colleagues from within the enterprise
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Follow-up activity	A process by which internal auditors evaluate the adequacy, effectiveness, and timeliness of actions taken by management on reported observations and recommendations, including those made by external auditors and others. Source: Institute of Internal Auditors—Practice Advisory 2500.A1-1; Copyright © by The Institute of Internal Auditors, Inc. All rights reserved.
Professional judgement	The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement

5. Effective Date

5.1 Effective Date This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

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!