IT AUDIT AND ASSURANCE GUIDELINE

G20 Reporting

The specialised nature of information technology (IT) audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards is a cornerstone of the ISACA professional contribution to the audit and assurance community. There are multiple levels of guidance:

- **Standards** define mandatory requirements for IT audit and assurance. They inform:
  - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow. The tools and techniques documents provide information on how to meet the standards when performing IT audit and assurance work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

COBIT® is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework's concepts. COBIT is intended for use by business and IT management as well as IT audit and assurance professionals; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. COBIT is available for download on the ISACA web site, *www.isaca.org/cobit*. As defined in the COBIT framework, each of the following related products and/or elements is organised by IT management process:

- Control objectives—Generic statements of minimum good control in relation to IT processes
- Management guidelines—Guidance on how to assess and improve IT process performance, using maturity models; Responsible, Accountable, Consulted and/or Informed (RACI) charts; goals; and metrics. They provide a management-oriented framework for continuous and proactive control self-assessment, specifically focused on:
  - Performance measurement
  - IT control profiling
  - Awareness
  - Benchmarking
- *COBIT Control Practices*—Risk and value statements and 'how to implement' guidance for the control objectives
- *IT Assurance Guide*—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met

A **glossary** of terms can be found on the ISACA web site at *www.isaca.org/glossary*. The words audit and review are used interchangeably in the IT Audit and Assurance Standards, Guidelines, and Tools and Techniques.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the audit and assurance professional should apply his/her own professional judgement to the specific circumstances presented by the particular systems or IT environment.

The ISACA Professional Standards Committee is committed to wide consultation in the preparation of the IT Audit and Assurance Standards, Guidelines, and Tools and Techniques. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Professional Standards Committee also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary. The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Any suggestions should be e-mailed (*standards@isaca.org*), faxed (+1.847. 253.1443) or mailed (address at the end of document) to ISACA International Headquarters, for the attention of the Val IT initiative manager. This material was issued on 16 August 2010.

1. BACKGROUND

1.1 Linkage to ISACA Standards

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

1.2 Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

- Control environment
- Information system
- Control procedures

1.3 Need for Guideline

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

2. INTRODUCTION

2.1. Purpose of This Guideline

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

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

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

3. ASSURANCE

3.1 Types of Services

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

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

3.2 Audit and Review

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

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

3.2.3 Both audits and reviews of control procedures involve:

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

- The conclusion for a review is expressed as a statement of negative assurance and provides only a moderate level of assurance.

3.3 Agreed-upon Procedures

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

3.4 Agreed-upon Procedures Reporting

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

- A title that includes the word independent
- Identification of the specified parties
- Identification of the subject matter (or the written assertion related thereto) and the type of engagement
- Identification of the responsible party
- A statement that the subject matter is the responsibility of the responsible party
- A statement that the procedures performed were those agreed to by the parties identified in the report
- A statement that the sufficiency of the procedures is solely the responsibility of the specified parties and a disclaimer of responsibility for the sufficiency of those procedures
- A list of the procedures performed (or reference thereto) and related findings
- A statement that the IT audit and assurance professional was not engaged in and did not conduct an examination of the subject matter
- A statement that if the IT audit and assurance professional had performed additional procedures, other matters might have come to the IT audit and assurance professional's attention and would have been reported
- A statement of restrictions on the use of the report because it is intended to be used solely by the specified parties

3.5 Engagement Mandate

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

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

4. IS AUDIT OPINION

4.1 Limitations

4.1.1 The IT audit and assurance professional's opinion is based on the procedures determined to be necessary for the collection of sufficient and appropriate evidence—that evidence being persuasive rather than conclusive in nature. The assurance provided by an IT audit and assurance professional

on the effectiveness of internal controls is, however, restricted because of the nature of internal controls and the inherent limitations of any set of internal controls and their operations. These limitations include:

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

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

4.2 Subsequent Events

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

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

4.3 Conclusions and Reporting

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

4.3.2 An IT audit and assurance professional's report about the effectiveness of control procedures should include the following elements:

- Title
- Addressee
- Description of the scope of the audit, the name of the entity or component of the entity to which the subject matter relates, including:
  - Identification or description of the area of activity
  - Criteria used as a basis for the IS audit and assurance professional's conclusion
  - The point in time or period of time to which the work, evaluation or measure of the subject matter relates

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

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

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

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

5. EFFECTIVE DATE

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

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *standards@isaca.org*
Web Site: *www.isaca.org*