IT AUDIT AND ASSURANCE GUIDELINE

G15 AUDIT PLANNING

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 controls professional should apply his/her own professional judgement to the specific control 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 1 March 2010.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning states that IT audit and assurance professionals should plan the information systems (IS) audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards. They should develop and document:

- A risk-based audit approach
- An audit plan that details the nature and objectives, timing and extent, objectives, and resources required
- An audit programme and/or plan detailing the nature, timing and extent of the audit procedures required to complete the audit

1.1.2 Standard S11 Use of Risk Assessment in Audit Planning states that IT audit and assurance professionals should:

- Use an appropriate risk assessment technique or approach in developing the overall IT audit plan and in determining priorities for the effective allocation of IT audit resources
- When planning individual reviews, identify and assess risks relevant to the area under review and its relationship to other auditable areas

1.1.3 Standard S12 Audit Materiality states that the IT audit and assurance professionals should consider:

- Audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures
- While planning for an audit, potential weaknesses or absences of controls and whether such weaknesses or absences of controls could result in significant deficiency or a material weakness in the information system
- The cumulative effect of minor control deficiencies or weaknesses and absences of controls to translate into significant deficiency or material weakness in the information system

1.2 Linkage to COBIT

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

1.2.3 Primary IT processes are:

- ME1 *Monitor and evaluate IT performance*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure compliance with external requirements*

1.2.4 Secondary IT process is:

- ME4 *Provide IT governance*

1.2.5 The information criteria most relevant are:

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

1.3 Need for Guideline

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

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

2. PRELIMINARY ENGAGEMENT ACTIVITIES

2.1 Purpose

2.1.1 The purpose of performing these preliminary engagement activities is to help ensure that IT audit and assurance professionals have considered any events or circumstances that may adversely affect their ability to plan and perform the audit engagement and reduce audit risk to an acceptably low level. Performing these preliminary engagement activities helps to ensure the audit engagement plans include that:

- IT audit and assurance professionals maintain the necessary independence and ability to perform the engagement
- There are no issues with management integrity that may affect IT audit and assurance professionals' willingness to continue the engagement
- There is no misunderstanding with the clients as to the terms of the engagement

2.2 Activities

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

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

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

3. PLANNING

3.1 Audit Strategy

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

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

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

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

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

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

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

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

3.2 Knowledge of the Enterprise

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

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

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

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

3.3 Materiality

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

3.4 Risk Assessment

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

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

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

3.5 Internal Control Evaluation

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

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

4. CHANGES DURING THE COURSE OF THE AUDIT

4.1 Strategy and Planning

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

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

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

5. SUPERVISION

5.1 Engagement Team Members

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

6. DOCUMENTATION

6.1 Planning Documentation

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

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

6.2 Plan Endorsement

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

6.3 Audit Programme

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

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

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

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

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

7. EFFECTIVE DATE

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

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*