IT AUDIT AND ASSURANCE GUIDELINE

G17 EFFECT OF NON-AUDIT ROLE ON THE IT AUDIT AND ASSURANCE PROFESSIONAL'S INDEPENDENCE

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

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

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

1.2 Linkage to COBIT

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

1.2.2 Primary IT processes are:

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

1.2.3 Secondary IT processes are:

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

1.2.4 The information criteria most relevant are:

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

1.3 Need for Guideline

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

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

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

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

1.3.3 Such non-audit roles are an important part of the IT audit and assurance professional's contribution

to the education and training of other members of the enterprise. They enable IT audit and assurance professionals to use their expertise and their knowledge of the enterprise to provide a unique and valuable contribution to the efficiency and effectiveness of the enterprise's IT investments. They also provide opportunities to raise the profile of the IT audit and assurance function and to give IT audit and assurance staff valuable practical experience.

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

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

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

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

2. AUDIT CHARTER

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

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

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

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

3 TYPES OF NON-AUDIT SERVICES

3.1. Involvements That Do Not Impair Independence

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

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

3.2 Involvements That Do Impair Independence

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

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

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

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

4. INDEPENDENCE

4.1 Relevance of Independence in Non-audit Roles

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

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

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

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

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

4.2 Effect of Non-audit Roles on Subsequent Audits

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

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

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

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

5. PLANNING

5.1 Effect on Independence

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

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

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

5.1.4 The IT audit and assurance professional should recommend actions or compensating controls that could be taken by the audit management/committee to provide reasonable assurance of independence and objectivity. These could include:

- Assigning additional management and/or staff from within the IT audit and assurance function who did not have any non-audit role in the area being audited, to supplement the IT audit and assurance professional who has/had a non-audit role
- Assigning management and staff from outside the IT audit and assurance function, such as borrowing staff from another function, division, external organisation, etc., to supplement the IT audit and assurance professional who has/had a non-audit role
- Assigning an independent resource, from within the IT audit and assurance function or other sources referenced previously, to carry out a peer review and to act as an independent arbiter during planning, field work and reporting

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

6. PERFORMANCE OF AUDIT WORK

6.1. Monitoring the Conduct of Audit

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

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

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

7. REPORTING

7.1 Disclosure Requirements

7.1.1 Where the independence of IT audit and assurance management and/or staff, with reference to an audit of an IS initiative and/or the related function, could be, or could appear to be, impaired by a non-audit role in the IS initiative, the IT audit and assurance professional should disclose in the audit report sufficient information about the non-audit role as well as the actions taken to provide reasonable assurance of independence and objectivity. This will enable the users of the audit report to understand the likely extent of the impairment, if any, and the measures taken to mitigate the effects of it. Information that IT audit and assurance professionals should consider disclosing includes aspects such as:

- Names and seniority of the IT audit and assurance management and staff involved in the IT initiative in non-audit roles
- Nature, timing and extent of their non-audit involvement in the IS initiative
- Reasons for their involvement in the non-audit role in the IS initiative as well as in the audit of the IS initiative or the related function
- Steps taken to provide assurance that independence and objectivity has not been materially impaired in the course of the audit work and the reporting process
- The fact that the potential impairment of independence has been highlighted to the audit committee or equivalent governance body and their agreement obtained before undertaking the non-audit role
- Existence and extent of the review undertaken to ensure the acceptable level of reliance on the work performed

8. EFFECTIVE DATE

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

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*