IS AUDITING GUIDELINE

# G7 DUE PROFESSIONAL CARE

The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IS auditing and reporting. They inform:
  - IS auditors 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 IS Auditing Standards. The IS auditor 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 IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.
- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

***Control Objectives for Information and related Technology* (COBIT®)** is an information technology (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 organisations. It emphasises regulatory compliance, helps organisations 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 IS auditors; 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 IS Auditing Standards, Guidelines and Procedures.

**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 Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board 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 director of research, standards and academic relations. This material was issued on 17 January 2008.

## 1. BACKGROUND

### 1.1 Linkage to Standards

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

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

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

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

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

### 1.2 Linkage to COBIT

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

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

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

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

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

**1.2.6** Secondary references:

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

**1.2.7** The information criteria most relevant are**:**

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

### 1.3 Need for Guideline

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

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

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

## 2. PERFORMANCE OF AUDIT WORK

### 2.1 Due Professional Care

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

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

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

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

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

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

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

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

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

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

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

## 3. EFFECTIVE DATE

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

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