IS AUDITING GUIDELINE

G5 AUDIT CHARTER

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 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 any 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 information technology 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 1 December 2007.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S1 Audit Charter states 'The responsibility, authority and accountability of the information systems audit function or information audit assignments should be appropriately documented in an audit charter or engagement letter'.

1.2 Linkage to COBIT

1.2.1 ME 4.7 *Independent assurance* states '…Provide the board with timely independent assurance about the compliance of IT with its policies, standards and procedures, as well as with generally accepted practices'.

1.2.2 ME 2.5 *Assurance of internal control* states 'Obtain, as needed, further assurance of the completeness and effectiveness on internal controls through third-party reviews'.

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to assist the IS auditor to prepare an audit charter to define the responsibility, authority and accountability of the IS audit function. This guideline is aimed primarily at the internal IS audit function; however, aspects could be considered for other circumstances.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

2. AUDIT CHARTER

2.1 Mandate

2.1.1 The IS auditor should have a clear mandate to perform the IS audit function. This mandate is ordinarily documented in an audit charter that should be formally accepted. Where an audit charter exists for the audit function as a whole, the IS audit mandate should be incorporated.

2.2 Contents of the Audit Charter

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

2.2.2 Purpose:

- Role
- Aims/goals
- Mission statement
- Scope
- Objectives

2.2.3 Responsibility:

- Operating principles
- Independence
- Relationship with external audit
- Auditee requirements
- Critical success factors
- Key performance indicators
- Risk assessment
- Other measures of performance

2.2.4 Authority:

- Right of access to information, personnel, locations and systems relevant to the performance of audits
- Scope or any limitations of scope
- Functions to be audited
- Auditee expectations
- Organisational structure, including reporting lines to board and senior management
- Grading of IS audit staff

2.2.5 Accountability:

- Reporting lines to senior management
- Assignment performance appraisals
- Personnel performance appraisals
- Staffing/career development
- Auditee rights
- Independent quality reviews
- Assessment of compliance with standards
- Benchmarking performance and functions
- Assessment of completion of the audit plan
- Comparison of budget to actual costs
- Agreed actions, e.g., penalties when either party fails to carry out their responsibilities

2.3 Communication With Auditees

2.3.1 Effective communication with auditees involves:

- Describing the service, its scope, its availability and timeliness of delivery
- Providing cost estimates or budgets if they are available
- Describing problems and possible resolutions for them
- Providing adequate and readily accessible facilities for effective communication
- Determining the relationship between the service offered and the needs of the auditee

2.3.2 The audit charter forms a sound basis for communication with auditees and should include references to service level agreements for such things as:

- Availability for unplanned work
- Delivery of reports
- Costs
- Response to auditee complaints
- Quality of service
- Review of performance
- Communication with auditees
- Needs assessment
- Control risk self-assessment
- Agreement of terms of reference for audits
- Reporting process
- Agreement of findings

2.4 Quality Assurance Process

2.4.1 The IS auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) to understand auditees' needs and expectations relevant to the IS audit function. These needs should be evaluated against the charter with a view to improving the service or changing the service delivery or audit charter, as necessary.

3. ENGAGEMENT LETTER

3.1 Purpose

3.1.1 Engagement letters are often used for individual assignments or for setting the scope and objectives of a relationship between external IS audit and an organisation.

3.2 Content

3.2.1 The engagement letter should clearly address the three aspects of responsibility, authority and accountability. Aspects to consider are set out in the following paragraphs.

3.2.2 Responsibility:

- Scope
- Objectives
- Independence
- Risk assessment

- Specific auditee requirements
- Deliverables

3.2.3 Authority:

- Right of access to information, personnel, locations and systems relevant to the performance of the assignment
- Scope or any limitations of scope
- Evidence of agreement to the terms and conditions of the engagement

3.2.4 Accountability:

- Intended recipients of reports
- Auditee rights
- Quality reviews
- Agreed completion dates
- Agreed budgets/fees if available

4. EFFECTIVE DATE

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

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