IS AUDITING GUIDELINE

G8 AUDIT DOCUMENTATION

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 S5 Planning, states ‘The IS auditor document an audit plan that lists the audit detailing the nature and objectives, timing and extent, objectives and resources required’.

1.1.2 Standard S6 Performance of Audit Work, states ‘During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence. The audit process should be documented, describing the audit work performed and the audit evidence that supports the IS auditor's findings and conclusions’.

1.1.3 Standard S7 Reporting, states ‘The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The audit 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, recommendations, and any reservations, qualifications or limitations that the IS auditor has with respect to the audit. When issued, the IS auditor’s report should be signed, dated and distributed according to the terms of the audit charter or engagement letter’.

1.1.4 Standard S12 Audit Materiality, states ‘The report of the IS auditor should disclose ineffective controls or absence of controls and the significance of the control deficiencies and possibility of these weaknesses resulting in a significant deficiency or material weakness’.

1.1.5 Standard S13 Using the Work of Other Experts, states ‘The IS auditor should determine whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives. Such conclusion should be clearly documented’.

1.2 Linkage to COBIT

1.2.1 PO1 *Define a strategic IT plan,* satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks by focusing on incorporating IT and business management in the translation of business requirements into service offerings and the development of strategies to deliver these services in a transparent and effective manner.

1.2.2 PO8 *Manage quality,* satisfies the business requirement for IT of continuous and measurable improvement of the quality of IT services delivered by focusing on the definition of a quality management system (QMS), ongoing performance monitoring against predefined objectives and implementation of a programme for continuous improvement of IT services.

1.2.3 AI6 *Manage changes,* satisfies the business requirement for IT of responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework by focusing on controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications, and halting implementation of unauthorised changes.

1.2.4 DS1 *Define and manage service,* satisfies the business requirement for IT of ensuring the alignment of key IT services with business strategy by focusing on identifying service requirements, agreeing on service levels and monitoring the achievement of service levels.

1.2.5 ME2 *Monitor and evaluate internal control,* satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws and regulations by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

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

1.2.7 The information criteria most relevant are:

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

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to describe the documentation that the IS auditor should prepare and retain to support the audit.

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 standards, use professional judgement in its application and be prepared to justify any departure.

2. PLANNING AND PERFORMANCE

2.1 Documentation Contents

2.1.1 IS audit documentation is the record of the audit work performed and the audit evidence supporting the IS auditor's findings, conclusions and recommendations. Audit documentation should be complete, clear, structured, indexed, and easy to use and understand by the reviewer. Potential uses of documentation include, but are not limited to:

- Demonstration of the extent to which the IS auditor has complied with the IS Auditing Standards
- Demonstration of audit performance to meet requirements as per the audit charter
- Assistance with planning, performance and review of audits
- Facilitation of third-party reviews
- Evaluation of the IS auditing function's QA programme
- Support in circumstances such as insurance claims, fraud cases, disputes and lawsuits
- Assistance with professional development of staff

2.1.2 Documentation should include, at a minimum, a record of:

- Review of previous audit documentation
- The planning and preparation of the audit scope and objectives. IS auditors must have an understanding of the industry, business domain, business process, product, vendor support and overall environment under review.
- Minutes of management review meetings, audit committee meetings and other audit-related meetings
- The audit programme and audit procedures that will satisfy the audit objectives
- The audit steps performed and audit evidence gathered to evaluate the strengths and weakness of controls
- The audit findings, conclusions and recommendations
- Any report issued as a result of the audit work
- Supervisory review

2.1.3 The extent of the IS auditor's documentation depends on the needs for a particular audit and should include such things as:

- The IS auditor's understanding of the areas to be audited and its environment.
- The IS auditor's understanding of the information processing systems and the internal control environment including the:
    - Control environment
    - Control procedures
    - Detection risk assessment
    - Control risk assessment
    - Equate total risk
- The author and source of the audit documentation and the date of its completion
- Methods used to assess adequacy of control, existence of control weakness or lack of controls, and identify compensating controls
- Audit evidence, the source of the audit documentation and the date of completion, including:
    - Compliance tests, which are based on test policies, procedures and segregation duties
    - Substantive tests, which are based on analytic procedures, detailed test accounts balances and other substantive audit procedures
- Acknowledgement from appropriate person of receipt of audit report and findings
- Auditee's response to recommendations
- Version control, especially where documentation is in electronic media

2.1.4 Documentation should include appropriate information required by law, government regulations or applicable professional standards.

2.1.5 Documentation should be submitted to the audit committee for its review and approval.

3. DOCUMENTATION

3.1 Custody, Retention and Retrieval

3.1.1 Policies and procedures should be in effect to verify and ensure appropriate custody and retention of the documentation that supports audit findings and conclusions for a period sufficient to satisfy legal, professional and organisational requirements.

3.1.2 Documentation should be organised, stored and secured in a manner appropriate for the media on which it is retained and should continue to be readily retrievable for a time sufficient to satisfy the policies and procedures defined above.

4. EFFECTIVE DATE

4.1. This revised 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
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*