IS AUDITING GUIDELINE

G13 USE OF RISK ASSESSMENT IN AUDIT PLANNING

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 published by the IT Governance Institute® (ITGI™). It 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 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 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 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 1 July 2008.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning states: ‘The IS auditor should plan the IS audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards’.

1.1.2 Standard S6 Performance of Audit Work states: ‘During the course of the audit, the IS auditor should obtain sufficient 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’.

1.1.3 Paragraph 2.4.1 of IS Auditing Guideline G15 Planning states: ‘An assessment of risk should be made to provide reasonable assurance that material items will be covered adequately during the audit work. This assessment should identify areas with relatively high risk of existence of material problems’.

1.2 Linkage to Procedures

1.2.1 This guideline may be used in conjunction with IS Auditing Procedure P1 IS Risk Assessment Measurement.

1.3 Linkage to COBIT

1.3.1 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 audit documentation requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary.

1.3.2 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.

1.3.2 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, regulations and contracts by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.3.5 Secondary references:

- ME3 *Ensure regulatory compliance*
- ME4 *Provide IT governance*

1.3.6 The information criteria most relevant are:

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

1.4 Need for Guideline

1.4.1 The level of audit work required to meet a specific audit objective is a subjective decision made by the IS auditor. The risk of reaching an incorrect conclusion based on the audit findings (audit risk) is one aspect of this decision. The other is the risk of errors occurring in the area being audited (error risk). Recommended practices for risk assessment in carrying out financial audits are well documented in auditing standards for financial auditors, but guidance is required on how to apply such techniques to IS audits.

1.4.2 Members of management also bases their decisions on how much control is appropriate upon assessment of the level of risk exposure that they are prepared to accept. For example, the inability to process computer applications for a period of time is an exposure that could result from unexpected and undesirable events (e.g., data centre fire). Exposures can be reduced by the implementation of appropriately designed controls. These controls are ordinarily based upon probabilistic estimation of the occurrence of adverse events and are intended to decrease such probability. For example, a fire alarm does not prevent fires, but it is intended to reduce the extent of fire damage.

1.4.3 This guideline provides guidance in applying IS Auditing Standards. The IS auditor should consider it in determining how to achieve implementation of standards S5 and S6, use professional judgement in its application, and be prepared to justify any departure.

2. PLANNING

2.1 Selection of a Risk Assessment Methodology

2.1.1 There are many risk assessment methodologies available from which the IS auditor may choose. These range from simple classifications of high, medium and low, based on the IS auditor's judgement, to complex and apparently scientific calculations to provide a numeric risk rating. IS auditors should consider the level of complexity and detail appropriate for the organisation being audited.

2.1.2 IS auditors should include, at a minimum, an analysis, within the methodology, of the risks to the enterprise resulting from the loss of and controls supporting system availability, data integrity and business information confidentiality.

2.1.3 All risk assessment methodologies rely on subjective judgements at some point in the process (e.g., for assigning weightings to the various parameters). The IS auditor should identify the subjective decisions required to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.

2.1.4 In deciding which is the most appropriate risk assessment methodology, IS auditors should consider such things as:

- The type of information required to be collected (some systems use financial effects as the only measure—this is not always appropriate for IS audits)
- The cost of software or other licences required to use the methodology
- The extent to which the information required is already available
- The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
- The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits
- The willingness of management to accept the methodology as the means of determining the type and level of audit work carried out

2.1.5 No single risk assessment methodology can be expected to be appropriate in all situations. Conditions affecting audits may change over time. Periodically, the IS auditor should re-evaluate the appropriateness of the chosen risk assessment methodologies.

2.2 Use of Risk Assessment

2.2.1 IS auditors should use the selected risk assessment techniques in developing the overall audit plan and in planning specific audits. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as:

- The nature, extent and timing of audit procedures
- The areas or business functions to be audited
- The amount of time and resources to be allocated to an audit

2.2.2 The IS auditor should consider each of the following types of risk to determine their overall level:

- Inherent risk
- Control risk
- Detection risk

2.3 Inherent Risk

2.3.1 Inherent risk is the susceptibility of an audit area to error in a way that could be material, individually or in combination with other errors, assuming that there were no related internal controls. For example, the inherent risk associated with operating system security is ordinarily high, since changes to, or even disclosure of, data or programs through operating system security weaknesses could result in false management information or competitive disadvantage. By contrast, the inherent risk associated with security for a stand-alone PC, when a proper analysis demonstrates it is not used for business-critical purposes, is ordinarily low.

2.3.2 Inherent risk for most IS audit areas is ordinarily high since the potential effects of errors ordinarily spans several business systems and many users.

2.3.3 In assessing the inherent risk, the IS auditor should consider both pervasive and detailed IS controls. This does not apply to circumstances where the IS auditor's assignment is related to pervasive IS controls only.

2.3.4 At the pervasive IS control level, the IS auditor should consider, to the level appropriate for the audit area in question:

- The integrity of IS management and IS management experience and knowledge
- Changes in IS management
- Pressures on IS management that may predispose them to conceal or misstate information (e.g., large business-critical project overruns, hacker activity)
- The nature of the organisation's business and systems (e.g., the plans for e-commerce, the complexity of the systems, the lack of integrated systems)
- Factors affecting the organisation's industry as a whole (e.g., changes in technology, IS staff availability)
- The level of third-party influence on the control of the systems being audited (e.g., because of supply chain integration, outsourced IS processes, joint business ventures, and direct access by customers)
- Findings from and date of previous audits

2.3.5 At the detailed IS control level, the IS auditor should consider, to the level appropriate for the audit area in question:

- The findings from and date of previous audits in this area
- The complexity of the systems involved
- The level of manual intervention required
- The susceptibility to loss or misappropriation of the assets controlled by the system (e.g., inventory, payroll)
- The likelihood of activity peaks at certain times in the audit period
- Activities outside the day-to-day routine of IS processing (e.g., the use of operating system utilities to amend data)
- The integrity, experience and skills of management and staff involved in applying the IS controls

2.4 Control Risk

2.4.1 Control risk is the risk that an error that could occur in an audit area and could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often missed easily, owing to the volume of logged information. The control risk associated with computerised data validation procedures is ordinarily low because the processes are consistently applied.

2.4.2 The IS auditor should assess the control risk as high unless relevant internal controls are:

- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

2.5 Detection Risk

2.5.1 Detection risk is the risk that the IS auditor's substantive procedures will not detect an error that could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with identifying a lack of disaster recovery plans is ordinarily low, since existence is verified easily.

2.5.2 In determining the level of substantive testing required, IS auditors should consider both:

- The assessment of inherent risk
- The conclusion reached on control risk following compliance testing

2.5.3 The higher the assessment of inherent and control risk the more audit evidence IS auditors should normally obtain from the performance of substantive audit procedures.

3. PERFORMANCE OF AUDIT WORK

3.1 Documentation

3.1.1 IS auditors should consider documenting the risk assessment technique or methodology used for a specific audit. The documentation should ordinarily include:

- A description of the risk assessment methodology used
- The identification of significant exposures and the corresponding risks
- The risks and exposures the audit is intended to address
- The audit evidence used to support the IS auditor’s assessment of risk

4. EFFECTIVE DATE

4.1 This guideline is effective for all IS audits beginning on or after 1 September 2000. The guideline has been reviewed and updated effective 1 August 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*