IS AUDITING GUIDELINE

G10 AUDIT SAMPLING

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 the 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.

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 July 2008.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 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’.

1.2 Linkage to COBIT

1.2.1 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 sampling requirement of IS auditors, 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 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.

1.2.3 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.

1.2.4 The primary references are:

- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*
- AI6 *Manage changes*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure regulatory compliance*

1.2.5 The information criteria most relevant are:

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

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to provide guidance to the IS auditor to design and select an audit sample and evaluate sample results. Appropriate sampling and evaluation will meet the requirements of ‘sufficient, reliable, relevant and useful evidence’ and ‘supported by appropriate analysis’.

1.3.2 The IS auditor should consider selection techniques that result in a statistically based representative sample for performing compliance or substantive testing.

1.3.3 Examples of compliance testing of controls, where sampling could be considered, include user access rights, program change control procedures, procedures documentation, program documentation, follow-up on exceptions, review of logs and software licences audits.

1.3.4 Examples of substantive tests, where sampling could be considered, include reperformance of a complex calculation (e.g., interest) on a sample of accounts, sample of transactions to vouch to supporting documentation, etc.

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

1.3.6 Other useful references on audit sampling include the International Standard on Auditing #530 Audit Sampling and Other Selective Testing Procedures, issued by the International Federation of Accountants (IFAC).

2. PERFORMANCE OF AUDIT WORK

2.1 Audit Sampling

2.1.1 When using either statistical or non-statistical sampling methods, the IS auditor should design and select an audit sample, perform audit procedures, and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence.

2.1.2 In forming an audit opinion, IS auditors frequently do not examine all of the information available as it may be impractical and valid conclusions can be reached using audit sampling.

2.1.3 Audit sampling is defined as the application of audit procedures to less than 100 percent of the population to enable the IS auditor to evaluate audit evidence about some characteristic of the items selected to form or assist in forming a conclusion concerning the population.

2.1.4 Statistical sampling involves the use of techniques from which mathematically constructed conclusions regarding the population can be drawn.

2.1.5 Non-statistical sampling is not statistically based, and results should not be extrapolated over the population as the sample is unlikely to be representative of the population.

2.2 Design of the Sample

2.2.1 When designing the size and structure of an audit sample, IS auditors should consider the specific audit objectives, the nature of the population, and the sampling and selection methods.

2.2.2 The IS auditor should consider the need to involve appropriate specialists in the design and analysis of samples.

2.2.3 The sampling unit depends on the purpose of the sample. For compliance testing of controls, attribute sampling is typically used, where the sampling unit is an event or transaction (e.g., a control such as an authorisation on an invoice). For substantive testing, variable or estimation sampling is frequently used where the sampling unit is often monetary.

2.2.4 The IS auditor should consider the specific audit objectives to be achieved and the audit procedures that are most likely to achieve those objectives. In addition, when audit sampling is appropriate, consideration should be given to the nature of the audit evidence sought and possible error conditions.

2.2.5 The population is the entire set of data from which the IS auditor wishes to sample to reach a conclusion on the population. Therefore, the population from which the sample is drawn has to be appropriate and verified as complete for the specific audit objective.

2.2.6 To assist in the efficient and effective design of the sample, stratification may be appropriate. Stratification is the process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum.

2.2.7 When determining sample size, the IS auditor should consider the sampling risk, the amount of the error that would be acceptable and the extent to which errors are expected.

2.2.8 Sampling risk arises from the possibility that the IS auditor's conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risk:

- The risk of incorrect acceptance—The risk that material misstatement is assessed as unlikely when, in fact, the population is materially misstated
- The risk of incorrect rejection—The risk that material misstatement is assessed as likely when, in fact, the population is not materially misstated

2.2.9 Sample size is affected by the level of sampling risk that the IS auditor is willing to accept. Sampling risk should also be considered in relation to the audit risk model and its components, inherent risk, control risk, and detection risk.

2.2.10 Tolerable error is the maximum error in the population that IS auditors are willing to accept and still conclude that the audit objective has been achieved. For substantive tests, tolerable error is related to the IS auditor's judgement about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the IS auditor is willing to accept.

2.2.11 If the IS auditor expects errors to be present in the population, a larger sample than when no error is expected ordinarily has to be examined to conclude that the actual error in the population is not greater than the planned tolerable error. Smaller sample sizes are justified when the population is expected to be error free. When determining the expected error in a population, the IS auditor should consider such matters as error levels identified in previous audits, changes in the organisation's procedures, and evidence available from an evaluation of the system of internal control and results from analytical review procedures.

2.3 Selection of the Sample

2.3.1 There are four commonly used sampling methods. Statistical sampling methods are:

- Random sampling—Ensures that all combinations of sampling units in the population have an equal chance of selection

- Systematic sampling—Involves selecting sampling units using a fixed interval between selections, the first interval having a random start. Examples include Monetary Unit Sampling or Value Weighted selection where each individual monetary value (e.g., $1) in the population is given an equal chance of selection. As the individual monetary unit cannot ordinarily be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weights the selection in favour of the larger amounts but still gives every monetary value an equal opportunity for selection. Another example includes selecting every 'nth sampling unit

Nonstatistical sampling methods are:

- Haphazard sampling—The IS auditor selects the sample without following a structured technique, while avoiding any conscious bias or predictability. However, analysis of a haphazard sample should not be relied upon to form a conclusion on the population
- Judgmental sampling—The IS auditor places a bias on the sample (e.g., all sampling units over a certain value, all for a specific type of exception, all negatives, all new users). It should be noted that a judgemental sample is not statistically based and results should not be extrapolated over the population as the sample is unlikely to be representative of the population.

2.3.2 The IS auditor should select sample items in such a way that the sample is expected to be representative of the population regarding the characteristics being tested, i.e., using statistical sampling methods. To maintain audit independence, the IS auditor should ensure that the population is complete and control the selection of the sample.

2.3.3 For a sample to be representative of the population, all sampling units in the population should have an equal or known probability of being selected, i.e., statistical sampling methods.

2.3.4 There are two commonly used selection methods: selection on records and selection on quantitative fields (e.g., monetary units). For selection on records, common methods are:

- Random sample (statistical sample)
- Haphazard sample (non-statistical)
- Judgemental sample (non-statistical; high probability to lead to a biased conclusion)

For selection on quantitative fields, common methods are:

- Random sample (statistical sample on monetary units)
- Fixed Interval sample (statistical sample using a fixed interval)
- Cell sample (statistical sample using random selection in an interval)

2.4 Documentation

2.4.1 The audit work papers should include sufficient detail to describe clearly the sampling objective and the sampling process used. The work papers should include the source of the population, the sampling method used, sampling parameters (e.g., random start number or method by which random start was obtained, sampling interval), items selected, details of audit tests performed and conclusions reached.

2.5 Evaluation of Sample Results

2.5.1 Having performed, on each sample item, those audit procedures which are appropriate to the particular audit objective, the IS auditor should analyse any possible errors detected in the sample to determine whether they are actually errors and, if appropriate, the nature and cause of the errors. For those that are assessed as errors, the errors should be projected as appropriate to the population, if the sampling method used, is statistically based.

2.5.2 Any possible errors detected in the sample should be reviewed to determine whether they are actually errors. The IS auditor should consider the qualitative aspects of the errors. These include the nature and cause of the error and the possible effect of the error on the other phases of the audit. Errors that are the result of the breakdown of an automated process ordinarily have wider implications for error rates than human error.

2.5.3 When the expected audit evidence regarding a specific sample item cannot be obtained, the IS auditor may be able to obtain sufficient, appropriate audit evidence by performing alternative procedures on the item selected.

2.5.4 The IS auditor should consider projecting the results of the sample to the population with a method of projection consistent with the method used to select the sampling unit. The projection of the sample may involve estimating the probable error in the population and estimating any further error that might not have been detected because of the imprecision of the technique together with the qualitative aspects of any errors found.

2.5.5 The IS auditor should consider whether errors in the population might exceed the tolerable error by comparing the projected population error to the tolerable error, taking into account the results of other audit procedures relevant to the audit objective. When the projected population error exceeds the tolerable error, the IS auditor should reassess the sampling risk and, if that risk is unacceptable, consider extending the audit procedure or performing alternative audit procedures.

3. EFFECTIVE DATE

3.1 This guideline is effective for all IS audits beginning on or after 1 March 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
E-mail: *standards@isaca.org*
Web Site: *www.isaca.org*