IS AUDITING GUIDELINE

G6 MATERIALITY CONCEPTS FOR AUDITING INFORMATION SYSTEMS

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 15 March 2008.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning states, 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.2 Standard S10 IT Governance, states 'The IS auditor should review and assess compliance with legal, environmental, information quality, fiduciary and security requirements'.

1.1.3 Standard S12 Audit Materiality, states 'The IS auditor should consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures. While planning for audit, the IS auditor should consider potential weakness or absence of controls and whether such weakness or absence of controls could result into significant deficiency or a material weakness in the information system. The IS auditor should consider the cumulative effect of minor control deficiencies or weaknesses and the absence of controls to translate into significant deficiency or material weakness in the information system'.

1.1.4 Standard S19 Irregularities and Illegal Acts, states 'If the IS auditor has identified a material irregularity or illegal act involving management or employees who have significant roles in internal control, or obtains information that a material irregularity or illegal act may exist, the IS auditor should communicate these matters to the appropriate level of management in a timely manner'.

1.2 Linkage to COBIT

1.2.1. PO5 *Manage the IT investment* 'satisfies the business requirement for IT of continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardised services that satisfy end-user expectations by focusing on effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions'.

1.2.2 AI1 *Identify automated solutions* 'satisfies the business requirement for IT of translating business functional and control requirements into an effective and efficient design of automated solutions by focusing on identifying technically feasible and cost-effective solutions'.

1.2.3 DS10 *Manage problems* 'satisfies the business requirement for IT of ensuring end users' satisfaction with service offerings and service levels; reducing solution and service delivery defects and rework by focusing on recording, tracking and resolving operational problems; investigating the root cause of all significant problems; and defining solutions for identified operations problems'.

1.2.4 DS13 *Manage operations* 'satisfies the business requirement for IT of maintaining data integrity and ensuring IT infrastructure can resist and recover from errors and failures by focusing on meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring and maintaining infrastructure'.

1.2.5 ME4 *Provide IT governance* 'satisfies the business requirement for IT of integrating IT governance with corporate governance objectives; complying with laws and regulations 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 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 materiality concept of auditing information systems by the IS auditor, the processes in COBIT most likely to be relevant, selected and adapted are classified as primary and secondary as follows. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.7 Secondary references:

- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI4 *Enable operation and use*
- AI5 *Procure IT resources*
- AI6 *Manage changes*
- DS3 *Manage performance and capacity*
- DS5 *Ensure systems security*
- DS9 *Manage the configuration*

- ME1 *Monitor and evaluate IT performance*
- ME2 *Monitor and evaluate internal control*

1.2.8 The information criteria most relevant to audit materiality are:
- Primary: Confidentiality, integrity, compliance, reliability
- Secondary: Effectiveness, efficiency, availability

2. NEED FOR GUIDELINE

2.1 IS vs. Financial Audits

2.1.1 Unlike financial auditors, IS auditors require a different yardstick to measure materiality. Financial auditors ordinarily measure materiality in monetary terms, since what they audit is also measured and reported in monetary terms. IS auditors ordinarily perform audits of non-financial items, e.g., physical access controls, logical access controls, program change controls, and systems for personnel management, manufacturing control, design, quality control, password generation, credit card production and patient care. Therefore, IS auditors may need guidance on how materiality should be assessed to plan their audits effectively, how to focus their effort on high-risk areas and how to assess the severity of any errors or weaknesses found.

2.1.2 This guideline provides guidance in applying IS auditing standards on audit materiality. 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.

3. PLANNING

3.1 Assessing Materiality

3.1.1 The assessment of what is material is a matter of professional judgement and includes consideration of the effect and/or the potential effect on the organisation's ability to meet its business objectives in the event of errors, omissions, irregularities and illegal acts that may arise as a result of control weaknesses in the area being audited.

3.1.2 While assessing materiality, the IS auditor should consider:
- The aggregate level of error acceptable to management, the IS auditor, appropriate regulatory agencies and other stakeholders
- The potential for the cumulative effect of small errors or weaknesses to become material

3.1.3 To meet the audit objectives, the IS auditor should identify the relevant control objectives and, based on risk tolerance rate, determine what should be examined. With respect to a specific control objective, a material control is a control or group of controls without which control procedures do not provide reasonable assurance that the control objective will be met.

3.1.4 Where the IS audit objective relates to systems or operations that process financial transactions, the financial auditor's measure of materiality should be considered while conducting the IS audit.

3.1.5 The IS auditor should determine establishment of roles and responsibilities as well as a classification of information assets in terms of confidentiality, availability and integrity; access control rules on privileges management; and classification of information based upon degree of criticality and risk of exposure. Assessment should include verification of:
- Information stored
- IS hardware
- IS architecture and software
- IS network infrastructure
- IS operations
- Development and test environment

3.1.6 The IS auditor should determine whether any IT general deficiency could potentially become material. The significance of such deficient IT general controls should be evaluated in relation to their effect on application controls, i.e., whether the associated application controls are also ineffective. If the application deficiency is caused by the IT general control, then they are material. For example, if an application-based tax calculation is materially wrong and was caused by poor change controls to tax tables, then the application-based control (calculation) and the general control (changes) are materially weak.

3.1.7 The IS auditor should evaluate an IT general control's deficiency in relation to its effect on application controls and when aggregated against other control deficiencies. For example, a management decision not to correct an IT general control deficiency and its associated reflection on the control

environment could become material when aggregated with other control deficiencies affecting the control environment.

3.1.8 The IS auditor should also note that failure to remediate a deficiency could become material.

3.1.9 The IS auditor should consider obtaining sign-off from appropriate stakeholders acknowledging they have disclosed existing material weakness that they are aware of in the organisation.

3.1.10 The following are examples of measures that should be considered to assess materiality:

- Criticality of the business processes supported by the system or operation
- Criticality of the information databases supported by the system or operation
- Number and type of application developed
- Number of users who use the information systems
- Number of managers and directors who work with the information systems classified by privileges
- Criticality of the network communications supported by the system or operation
- Cost of the system or operation (hardware, software, staff, third-party services, overheads or a combination of these)
- Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage, etc.)
- Cost of loss of critical and vital information in terms of money and time to reproduce
- Effectiveness of countermeasures
- Number of accesses/transactions/inquiries processed per period
- Nature, timing and extent of reports prepared and files maintained
- Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)
- Service level agreement requirements and cost of potential penalties
- Penalties for failure to comply with legal, regulatory and contractual requirements
- Penalties for failure to comply with public health and safety requirements

3.1.11 Control failures may potentially lead to monetary loss, competitive position, loss of trust or loss of reputation, apart from damaging the corporate image. The IS auditor should evaluate risks against possible countermeasures.

4. REPORTING

4.1 Identifying Reportable Issues

4.1.1 In determining the findings, conclusions and recommendations to be reported, the IS auditor should consider both the materiality of any errors found and the potential materiality of errors that could arise as a result of control weaknesses.

4.1.2 Where the audit is used by management to obtain a statement of assurance regarding IS controls, an unqualified opinion on the adequacy of controls should mean that the controls in place are in accordance with generally accepted control practices to meet the control objectives, devoid of any material control weakness.

4.1.3 A control weakness should be considered material and, therefore, reportable, if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. If the audit work identifies material control weaknesses, the IS auditor should consider issuing a qualified or adverse opinion on the audit objective.

4.1.4 Depending on the objectives of the audit, the IS auditor should consider reporting to management weaknesses that are not material, particularly when the costs of strengthening the controls are low.

5. EFFECTIVE DATE

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

2007-2008 ISACA STANDARDS BOARD

Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Capco IT Services India Private Ltd., India
Brad David Chin, CISA, CPA	Google Inc., USA
Sergio Fleginsky, CISA	AKZO Nobel, Uruguay
Maria Gonzalez, CISA, CISM	Department of Defence, Spain
John Ho Chi, CISA, CISM, CBCP, CFE	Ernst & Young, Singapore
Andrew J. MacLeod, CISA, CIA, FCPA, MACS, PCP	Brisbane City Council, Australia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Jason Thompson, CISA	KPMG LLP, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA	Microsoft Corp., USA

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*