IS AUDITING GUIDELINE

G4 OUTSOURCING OF IS ACTIVITIES TO OTHER ORGANISATIONS

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 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 15 March 2008.

1. BACKGROUND

1.1 Linkage to Standards

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

1.1.2 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’.

1.1.3 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 Guidelines

1.2.1 Guideline G16 sets out how the IS auditor should comply with the ISACA IS Auditing Standards and COBIT when assessing the effect a third party has on an organisation's IS controls and related control objectives.

1.3 Linkage to COBIT

1.3.1 DS2 *Manage third-party services* states that the IS auditor should establish what controls the service user has put in place to address the business requirement to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements.

1.4 Need for Guideline

1.4.1 An organisation (the service user) may partially or fully delegate some or all of its IS activities to an external provider of such services (the service provider). The provider could either be onsite using the service user’s systems or offsite using its own systems. IS activities that could be outsourced include IS functions such as data centre operations, security, and application system development and maintenance.

1.4.2 The responsibility for confirming compliance with contracts, agreements and regulations remains with the service user.

1.4.3 The rights to audit are often unclear. The responsibility for auditing compliance is also often not clear. The purpose of this guideline is to set out how the IS auditor should comply with standards S1, S5 and S6 in this situation.

1.4.4 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. AUDIT CHARTER

2.1 Responsibility, Authority and Accountability

2.1.1 Where any aspect of the IS function has been outsourced to a service provider, these services should be included in the scope of the audit charter.

2.1.2 The audit charter should explicitly include the right of the IS auditor to:

- Review the agreement between the service user and the service provider (pre- or post-effect)
- Carry out such audit work as is considered necessary regarding the outsourced function
- Report findings, conclusions and recommendations to service user management

3. PLANNING

3.1 Fact Finding

3.1.1 The IS auditor should obtain an understanding of the nature, timing and extent of the outsourced services.

3.1.2 The risks associated with the outsourced services should be identified and assessed.

3.1.3 The IS auditor should assess the extent to which the service user’s controls provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

3.1.4 The IS auditor should obtain an understanding of which controls are the responsibility of the service provider (or additional subcontracted third parties) and which controls will remain the responsibility of the service user.

3.1.5 The IS auditor should determine the extent to which the outsource agreement provides for the audit of the service provider and consider whether this provision is adequate. This includes assessing the potential reliance on any IS audit work carried out by either the service provider's internal auditors or an independent third party contracted by the service provider.

3.2 Planning

3.2.1 The IS auditor should consider obtaining appropriate expert legal advice when reviewing the contract and service level agreement (SLA) during the planning phase for the extent and any stipulations regarding the right to audit the service provider.

3.2.2 The IS auditor should evaluate any previous audit report prepared for the service provider and plan the IS audit work to address the audit objectives relevant to the service provider's environment, taking into account the information obtained during planning.

3.2.3 The IS auditor should consider what type of outsourcing has been used and what impact it will have on the audit approach:

- Labor outsourcing (common offshore model):
  - Only the labor is outsourced. The service user's internal controls and business processes remain the same. The service provider relies completely on the service user's IT environment to deliver the service.
  - The IS auditor should plan on testing the service user's existing IT controls as well as any additional controls that support that SLA.
- Labor and systems outsourcing (common onshore model):
  - The service provider uses its own IT environment to deliver the service (e.g., payroll outsourcing).
  - The IS auditor should consider whether the service provider is able to provide any documentation of controls testing performed by qualified independent third parties (e.g., SAS70 Type II report) and whether the objectives covered in the testing are applicable to the IS auditor's audit objectives

3.2.4 The audit objectives should be agreed upon with the service user management before being communicated to the service provider. Any changes requested by the service provider should be agreed with the service user management.

3.2.5 The IS auditor should consider the international certifications or frameworks and also International Organization on Standardization requirements that would apply to outsourcing, while deciding the scope and objectives of the work. Based on that, the IS auditor should decide the extent to which international certifications obtained by the service organisation can be relied upon.

3.2.6 The IS auditor should plan the IS audit work to comply with applicable professional audit standards, as if the audit were performed in the service user's own environment.

4. PERFORMANCE OF AUDIT WORK

4.1 Audit Evidence Requirement

4.1.1 The audit should be performed as if the service was being provided in the service user's own IS environment.

4.2 The Agreement With the Service Provider

4.2.1 The IS auditor should consider such things as:

- Existence of a formal agreement between the service provider and the service user
- Inclusion in the outsourcing agreement of a clause that explicitly states that the service provider is obligated to meet all legal requirements applying to its activities and comply with acts and regulations pertaining to the functions it undertakes on behalf of the service user
- Specific and enforceable stipulations in the outsourcing agreement that activities performed by the service provider are subject to controls and audits as if they were performed by the service user itself

- Inclusion of audit access rights in the agreement with the service provider including both the internal audit staff from the service user and any third parties conducting audits of the service user
- Inclusion of provisions requiring the service provider to monitor compliance with the SLA and proactively report any incidents or failures of controls
- Existence of SLAs with performance monitoring procedures
- Adherence to the service user's security policies
- Adequacy of the service provider's fidelity insurance arrangements
- Adequacy of the service provider's personnel policies and procedures, including segregation of duties between key tasks
- Adequacy of the service provider's policies and procedures for subcontracting tasks to additional third parties and monitoring of SLA performance by those providers
- Adequacy of service provider's ability to continue operations in the event of a disaster

4.3 Management of Outsourced Services

4.3.1 The IS auditor should verify that:

- Business processes to produce the information used to monitor compliance with the SLAs are appropriately controlled. The service user should have either accepted the standard service level compliance information available from the service provider or added additional reporting requirements that have been agreed to by the service provider.
- Where SLAs are not being met, the service user has sought remedy and corrective actions have been considered to achieve the agreed-to service level
- The service user has the capacity and competence to follow up and review the services provided

4.4 Restrictions on Scope

4.4.1 Where the service provider proves unwilling to co-operate with the IS auditor, the IS auditor should report the matter to the service user's management. This may also include operations that have been subcontracted by the service provider to additional third parties without a right-to-audit provision in the contract.

5. REPORTING

5.1 Issuing and Agreeing the Report

5.1.1 The IS auditor should provide a report in an appropriate form to the intended service user recipients upon the completion of the audit work.

5.1.2 The IS auditor should consider discussing the report with the service provider prior to release, but the IS auditor should not be responsible for issuing the final report to the service provider. If the service provider is to receive a copy, this should ordinarily come from the service user's management.

5.1.3 The report should specify any restrictions on distribution that the IS auditor or service user management have agreed to impose. For example, the service provider should not be able to provide a copy of the report to other users of their service without the permission of the IS auditor's organisation and, where appropriate, the service user. The IS auditor should also consider including a statement excluding liability to third parties.

5.2 Reporting Restrictions on Scope

5.2.1 The audit report should clearly identify a restriction on scope where audit access rights are denied and should explain the effect of this restriction with respect to the audit.

6. FOLLOW-UP ACTIVITIES

6.1 Effect of Previous Audits

6.1.1 As if the audit had been performed in the service user's own environment, the IS auditor should request appropriate information from both the service user and the service provider on previous relevant findings, conclusions and recommendations. The IS auditor should determine whether appropriate corrective actions have been implemented by the service provider in a timely manner.

7. EFFECTIVE DATE

7.1 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.

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*