Serving IT Governance Professionals

IS AUDITING GUIDELINE

G11 EFFECT OF PERVASIVE IS CONTROLS

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

1.2.2 Primary references:

- PO4 *Define IT processes, organisation and relationships*
- AI4 *Enable operation and use*
- AI6 *Manage changes*
- AI7 *Install and accredit solutions and changes*

1.2.3 Secondary references:

- DS3 *Manage performance and change*
- DS5 *Ensure system security*
- ME2 *Monitor and evaluate internal control*

1.2.4 The information criteria most relevant are:

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

1.3 Need for Guideline

1.3.1 The management and monitoring of any organisation, department or function has an affect on the way in which that organisation, department or function behaves, including the way in which it applies controls. This principle applies as much to the use of IS as it does to a manufacturing organisation, an accounts payable department or a treasury function.

1.3.2 The effectiveness of the detailed IS controls operated within an organisation is limited by the effectiveness of the management and monitoring of the use of information systems in the organisation as a whole. This is often recognised in guidelines for financial audits, where the effect of 'general' controls in the IS environment on 'application' controls in the financial systems is acknowledged.

1.3.3 The IT Governance Institute's COBIT framework can assist the IS auditor in differentiating between:

- The detailed IS controls that are directly relevant to the IS audit scope
- The features of IS management and monitoring that contribute to the assurance and may be obtained by an IS auditor in relation to those detailed IS controls

1.3.4 The general/application control split was designed specifically to apply to audits whose objective is to form an opinion on data processing integrity, system availability to business users and business information confidentiality.

1.3.5 When internal auditors and independent consultants perform IS audits, the audit objective and scope are ordinarily different from those for business processes including financial audits. The systems in use are a combination of manual and computer processes, and the control objectives must be for the entire process, which may be either wider or narrower than business processes including accounting information records. Therefore, the controls framework used for business process audits may not be appropriate for some IS audits.

1.3.6 To form an opinion on the effectiveness of the detailed controls being audited, the IS auditor should consider the need to assess the effectiveness of management and monitoring of information systems, even where such matters are outside the agreed-upon scope for the audit. The outcome of such considerations may range from an extension of the agreed scope to an appropriately qualified report.

1.3.7 The total population of management and monitoring controls is broad, and some of these controls may not be relevant to the specific audit objective. To assess the audit risk and determine the appropriate audit approach, the IS auditor needs a structured method of determining:

- Those management and monitoring controls that are relevant to the audit scope and objectives
- Those management and monitoring controls that should be tested
- The effect of the relevant management and monitoring controls on the audit opinion

This may be achieved using a framework of controls specific to the use of IS and related technology, which may help the IS auditor to focus on the key controls that affect the information systems and operations being audited.

1.3.8 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.

2. CONTROLS FRAMEWORK

2.1 Overview

2.1.1 COBIT defines control as 'The policies, procedures, practices and organisational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected'. For each IS audit, the IS auditor should differentiate between those general controls which affect all information systems and operations (pervasive IS controls) and those general and application controls that operate at a more specific level (detailed IS controls) to focus audit effort on the risk areas relevant to the IS audit objective. The purpose of the controls framework described in this section is to assist the IS auditor in achieving this focus.

2.2 Pervasive IS Controls

2.2.1 The term 'pervasive IS controls' is defined in the ISACA glossary at *www.isaca.org/glossary.* Pervasive IS controls are a subset of general controls; they are those general controls that focus on the management and monitoring of IS.

2.2.2 The effect of pervasive IS controls on the IS auditor's work is not limited to the reliability of application controls in the business process systems. Pervasive IS controls also affect the reliability of the detailed IS controls over, for example:

- Application program development
- System implementation
- Security administration
- Backup procedures

2.2.3 Weak management and monitoring of IS (i.e., weak pervasive IS controls) should alert the IS auditor to the possibility of a high risk that the controls designed to operate at the detailed level may be ineffective.

2.2.4 Pervasive controls are most effectively determined via a risk assessment where crucial processes and controls are identified. For example, depending upon the organisation, the risk assessment may result in rating the controls (i.e., segregation of duties) around the evaluation of program changes from the testing environment into the production processing environment. Specifically, controls that segregate the program development and change environment from the production process environment may be considered pervasive controls. The means and method of accomplishing this control objective ensures that the elevation of new or modified programs is performed by those individuals typically assigned to the production processing environment. Accordingly, pervasive controls are essential to the reliance placed upon other detailed controls.

2.3 Detailed IS Controls

2.3.1 The term detailed IS controls is defined in the ISACA glossary at *www.isaca.org/glossary*. They are made up of application controls plus those general controls not included in pervasive IS controls. In the COBIT framework, detailed IS controls are the controls over the acquisition, implementation, delivery and support of IS systems and services. Examples include controls over:

- Implementation of software packages
- System security parameters
- Disaster recovery planning
- Data input validation
- Exception report production

- User accounts

Application controls are a subset of detailed IS controls. Data input validation, for example, is both a detailed IS control and an application control. AI7 *Install and accredit solutions and changes* is an IS control, but not an application control.

2.3.2 The relationships amongst IS controls are shown in the following outline:

IS Controls

→ General controls
  - Pervasive IS controls
  - Detailed IS controls

→ Application controls

In addition, the IS auditor should consider the effect of non-IS controls on scope and audit procedures.

2.4 Interaction of Pervasive and Detailed IS Controls

2.4.1 Pervasive controls should be analysed based upon the four domains in COBIT:

- Plan and Organise (PO)
- Acquire and Implement (AI)
- Deliver and Support (DS)
- Monitor and Evaluate (ME)

2.4.2 Pervasive controls should be identified from the risks associated with the loss of system availability, data integrity and information confidentiality. For example, controls prohibiting unauthorised and consequential update, which will go undetected, to production data used in either financial or non-financial reporting of a publicly traded company may be construed as a pervasive control from a data-integrity perspective. The remaining parts of 2.4 further illustrate potential pervasive controls in each of the domains.

2.4.3 The effectiveness of the controls in the AI and DS domains is influenced by the effectiveness of the controls operated in the PO and ME domains. Inadequate planning, organisation and monitoring by management imply that controls over acquisition, implementation, and service delivery and support will be ineffective. Conversely, strong planning, organisation and monitoring can identify and correct ineffective controls over acquisition, implementation, and service delivery and support.

2.4.4 For example, detailed IS controls over the COBIT process AI2 *Acquire and maintain application software* include the following COBIT processes:

- PO1 *Define a strategic IT plan*
- PO8 *Manage quality*
- PO10 *Manage projects*
- ME1 *Monitor and evaluate IT performance*

2.4.5 An audit of an application system acquisition should include the identification of the effect of the IS strategy, the project management approach, quality management and the approach to monitoring. Where, for example, project management is inadequate, the IS auditor should consider:

- Planning additional work to provide assurance that the specific project being audited is being effectively managed
- Reporting weaknesses in pervasive IS controls to management

2.4.6 A further example is that effective detailed IS controls over the COBIT process DS5 *Ensure systems security* are affected by the adequacy of pervasive IS controls over processes including the following COBIT processes:

- PO4 *Define the IT processes, organisation and relationships*
- PO6 *Communicate management aims and direction*
- PO9 *Assess and manage IT risks*
- ME1 *Monitor and evaluate IT performance*

2.4.7 An audit of the adequacy of security parameters in a system should include consideration of management's security policies (PO6), allocation of security responsibilities (PO4), risk assessment procedures (PO9) and procedures for monitoring compliance with its security policies (ME1). Even where the parameters do not comply with the IS auditor's view of best practice, they may be evaluated as adequate in light of the risks identified by management and the management policies that direct how such a level of risk should be addressed. Any audit recommendations for improvement, as well as the detailed parameters themselves, should then be directed to risk management.

3. PLANNING

3.1 Approach to Relevant Pervasive IS Controls

3.1.1 The IS Auditing Guideline G15 Planning states that the IS auditor should perform a preliminary assessment of control over the function being audited. A risk assessment is essential in identifying and evaluating relevant pervasive IS controls. The testing of pervasive IS controls may take place on a different cycle to the specific IS audit being performed, since, by their nature, they cover many different aspects of IS usage. The IS auditor should, therefore, consider whether any previous audit work in this area could be relied upon to identify and evaluate these controls.

3.1.2 Where audit work indicates that pervasive IS controls are unsatisfactory, the IS auditor should consider the effect of this finding on the planned approach to achieving the audit objective:

- Strong pervasive IS controls can contribute to the assurance that may be obtained by an IS auditor in relation to detailed IS controls.
- Weak pervasive IS controls may undermine strong detailed IS controls or exacerbate weaknesses at the detailed level.

3.2 Sufficient Audit Procedures

3.2.1 Where pervasive IS controls have a significant potential effect on the audit objective, it is not sufficient to plan to audit only the detailed controls. Where it is not possible or practical to audit the pervasive IS controls, this restriction of scope should be reported.

3.2.2 The IS auditor should plan to test the relevant pervasive IS controls, where this test will contribute to achieving the audit objective.

3.3 Relevant Controls

3.3.1 Relevant pervasive IS controls are those that have an effect on the specific audit objectives for the assignment. For example, where the audit objective is to report on the controls around changes to a specific programme library, pervasive IS controls relating to security policies (PO6) will be relevant, but pervasive IS controls relating to determination of the technological direction (PO3) may not be relevant.

3.3.2 In planning the audit, the IS auditor should identify which of the total population of pervasive IS controls have an effect on the specific audit objectives, and should plan to include these in the audit scope. COBIT's control objectives for the PO and ME domains may help the IS auditor to identify relevant pervasive IS controls.

3.4 Audit Evidence

3.4.1 The IS auditor should plan to obtain audit evidence that relevant controls are operating effectively. Potential tests are outlined in section 4, Performance of Audit Work.

3.5 Approach to Relevant Detailed IS Controls

3.5.1 Where IS audit work indicates that pervasive IS controls are satisfactory, the IS auditor may consider reducing the level of testing planned for detailed IS controls, since the audit evidence of strong pervasive IS controls will contribute to the assurance that may be obtained by an IS auditor in relation to detailed IS controls.

3.5.2 Where IS audit work indicates that pervasive IS controls are not satisfactory, the IS auditor should carry out sufficient testing of detailed IS controls to provide audit evidence that they are working effectively in spite of weaknesses in the relevant pervasive IS controls.

4. PERFORMANCE OF AUDIT WORK

4.1. Testing Pervasive IS Controls

4.1.1 The IS auditor should carry out sufficient testing to provide assurance that relevant pervasive IS controls were operating effectively in the audit period or at a specific point in time. Test procedures that may be appropriate include:

- Observation
- Corroborative inquiries

- Review of relevant documentation (e.g., policies, standards, meeting minutes)
- Reperformance (e.g., using CAATs)

4.1.2 If the testing of the relevant pervasive IS controls indicates that they are satisfactory, the IS auditor should proceed with the planned audit of the detailed IS controls that are directly applicable to the audit objective. The level of such testing may be less than would be appropriate if the pervasive IS controls were not operating satisfactorily.

5. REPORTING

5.1 Pervasive IS Control Weaknesses

5.1.1 Where the IS auditor has identified weaknesses in pervasive IS controls, these should be brought to the attention of management, even where consideration of such areas was not specifically identified in the agreed-upon scope of work.

5.2 Restrictions on Scope

5.2.1 Where pervasive IS controls could have a significant potential effect on the effectiveness of detailed IS controls and the pervasive IS controls have not been audited, the IS auditor should bring this fact to the attention of management in the final report, together with a statement of the potential effect on the audit findings, conclusions and recommendations. For example, when an IS auditor is reporting on an audit of the acquisition of a package solution, but has not seen the organisation's IS strategy, the IS auditor should include in the report a statement that the IS strategy has not been made available or does not exist. Where relevant, the IS auditor should go on to report the potential effect on the audit findings, conclusions and recommendations, e.g., through a statement that it is not possible to say whether the acquisition of the package solution is consistent with the IS strategy and will support the future plans of the business.

6. EFFECTIVE DATE

6.1 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*