Introduction—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 Information Systems Audit and Control Association™ (ISACA®) is to advance globally applicable standards to meet this need. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community.

Objectives—The objectives of the ISACA IS Auditing Standards are to 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 for IS auditors
- Management and other interested parties of the profession’s expectations concerning the work of practitioners

The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.

Scope and Authority of IS Auditing Standards—The framework for the IS Auditing Standards provides multiple levels of guidance:
- Standards define mandatory requirements for IS auditing and reporting.
- 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 judgment in their application and be prepared to justify any departure.
- Procedures provide examples of procedures an IS auditor might follow in an audit engagement. Procedures should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtain the same results. In determining the appropriateness of any specific procedure, group of procedures or test, IS auditors should apply their own professional judgment to the specific circumstances presented by the particular information systems or technology environment. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements.

The words audit and review are used interchangeably. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.htm.

Holders of the Certified Information Systems Auditor™ (CISA®) designation are to comply with IS Auditing Standards adopted by ISACA. 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.

Development of Standards, Guidelines and Procedures—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 following CoEIT® resources should be used as a source of best practice guidance:
- Control Objectives—High-level and detailed generic statements of minimum good control
- Control Practices—Practical rationales and how-to-implement guidance for the control objectives
- Audit Guidelines—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
- Management Guidelines—Guidance on how to assess and improve IT process performance, using maturity models, metrics and critical success factors

Each of these is organised by the IT management process, as defined in the CoEIT Framework. CoEIT is intended for use by businesses and IT management as well as IS auditors. Its usage enables the understanding of business objectives and for the communication of best practices and recommendations around a commonly understood and well-respected standard reference.

The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to help identify emerging issues requiring new standards. Any suggestions should be e-mailed (research@isaca.org), faxed (+1.847.253.1443) or mailed (address at the end of this guideline) to ISACA International Headquarters, for the attention of the director of research standards and academic relations.

This material was issued on 1 May 2003.
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."

1.1.2 Guideline G14 Review of Application Systems provides guidance.
1.1.3 Guideline G17 Effect of Nonaudit Roles on the IS Auditor’s Independence provides guidance.
1.1.4 Guideline G20 Reporting provides guidance.

1.2 Linkage to COBIT®
1.2.1 The COBIT Framework states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."
1.2.2 The COBIT Management Guidelines provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
   - Performance measurement—How well is the IT function supporting business requirements?
   - IT control profiling—What IT processes are important? What are the critical success factors for control?
   - Awareness—What are the risks of not achieving the objectives?
   - Benchmarking—What do others do? How can results be measured and compared?
1.2.3 The Management Guidelines provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.
1.2.4 The Management Guidelines can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. 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 information criteria.
1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Guideline
1.3.1 To support the business operations, organisations implement application systems. The process of defining, acquiring and implementing application systems involves various stages from identifying requirements to actually implementing the application system and generally is referred to as a system development life cycle (SDLC).
1.3.2 This guideline is meant to provide the necessary guidance to IS auditors in carrying out reviews of the SDLC of application systems.

2. SYSTEMS DEVELOPMENT LIFE CYCLE

2.1 Definition
2.1.1 The system development life cycle is the process, involving multiple stages (from establishing the feasibility to carrying out post implementation reviews), used to convert a management need into an application system, which is custom-developed or purchased or is a combination of both.

2.2 Factors Influencing the SDLC
2.2.1 The SDLC for an application system would depend on the chosen acquisition/development mode. Application systems could be acquired/developed through various modes, which include:
   - Custom development using internal resources
   - Custom development using fully or partly outsourced resources located onsite or offsite (locally or in an offshore location)
   - Vendor software packages implemented as-is with no customisation
   - Vendor software packages customised to meet the specific requirements

At times, large complex applications may involve a combination of the above.
2.2.2 Some organisations use specific SDLC methodologies and processes, either custom- or vendor-developed. These generally prescribe standard processes for different modes of acquisition with the facility to customise the process design for specific application systems. These may be supported by appropriate tools to manage the SDLC. In such cases, the SDLC would depend on the methodology/tool.
2.2.3 Where an application system is developed instead of being purchased as a package, the SDLC would depend on the development methodology used, such as waterfall development, prototyping, rapid application development, CASE and object-oriented development.

2.3 SDLC Risks
2.3.1 During the SDLC of an application system, various risks could be encountered, which include:
   - Adoption of inappropriate SDLC for the application system
   - Inadequate controls in the SDLC process
   - User requirements and objectives not being met by the application system
Inadequate stakeholder (including internal audit) involvement
Lack of management support
Inadequate project management
Inappropriate technology and architecture
Scope variations
Time over-runs
Cost over-runs
Inadequate quality of the application system
Insufficient attention to security and controls (including validations and audit trails) in the application system
Performance criteria not being met
Inappropriate resourcing/staffing model management
Inadequate staffing skills
Insufficient documentation
Inadequate contractual protection
Inadequate adherence to chosen SDLC and/or development methodologies
Insufficient attention to interdependencies on other applications and processes
Inadequate configuration management
Insufficient planning for data conversion/migration and cutover
Post cut-over disruption to business

3. PLANNING

3.1 Factors to be Considered in Planning
3.1.1 The IS auditor should consider the following while planning the review of the SDLC of an application system:
- The acquisition/development mode, technology, size, objectives and intended usage of the application system
- Project structure for the acquisition and implementation
- Skill and experience profile of the project team
- The SDLC model chosen
- The formal SDLC methodology and customised process design adopted, if any
- Risks that are likely to effect the SDLC
- Any concerns or issues perceived by appropriate management
- The current SDLC stage
- Any prior review of the earlier SDLC stages of the application system
- Any prior SDLC reviews of similar application systems
- Any other risk assessments/reviews by the IS auditor or others (such as IT) that have a bearing on the proposed review
- The skill and experience level of the IS auditors available and the possibility of getting competent external assistance where necessary

3.2 Terms of Reference
3.2.1 Taking the above into account, the IS auditor should arrive at the terms of reference (TOR) of the planned SDLC review. This should include:
- The objectives of the review
- Scope of the review in terms of SDLC stages to be covered by the review
- Type of review—whether it is a pre-implementation review of the proposed SDLC, a parallel/concurrent review as the SDLC stages are being executed, or a post-implementation review after the SDLC stages in question are completed
- The timeframe of the review—likely start and end dates
- Process for reporting the observations and recommendations
- Process for following up on the agreed actions

3.2.2 The IS auditor should obtain the agreement of the appropriate management for the proposed review of the SDLC of the chosen application system.

4. COMPETENCE

4.1 Skills and Experience
4.1.1 The IS auditors assigned to the SDLC review should have the requisite skills and experience to carry out the review cost-effectively and efficiently. Where specific SDLC methodologies and tools are used, the IS auditors should possess adequate knowledge and experience regarding such methodologies and tools and the associated risks. Similarly, where the application system is being developed instead of being purchased from a vendor, the IS auditor should possess sufficient knowledge and experience regarding the development methodologies and tools being used (such as waterfall development, prototyping, rapid application development, CASE and object-oriented development). If warranted, the IS auditor should seek external resources (subject to applicable policies, procedures and approvals) to complement the internal skill availability.

5. INDEPENDENCE

5.1 Independence
5.1.1 When reviewing the SDLC of application systems, the IS auditor should be, and be seen to be, independent of the project team responsible for acquiring and implementing the application system. Guideline G17, which provides guidance regarding the Effect of Nonaudit Roles on the IS Auditor’s Independence, should be considered in this context.
6. PERFORMANCE OF REVIEW WORK

6.1 Types of Reviews

6.1.1 The IS auditor should carry out the review or audit of the SDLC as per the TOR agreed upon with the appropriate management:
- Where the review is a pre-implementation review, the IS auditor should study the proposed SDLC model and the related aspects to assess their appropriateness as well as the potential risks and provide the necessary risk mitigation recommendations to the appropriate management.
- In the case of parallel/concurrent reviews, the IS auditor should review the relevant SDLC stages, as they are happening, to highlight risks/issues and provide necessary risk mitigation recommendations to the appropriate management.
- In the case of post-implementation reviews, the IS auditor should review the relevant SDLC stages after their completion to highlight issues faced and provide recommendations for downstream corrections (if possible) and to serve as a learning tool for the future.

6.2 Aspects to be Reviewed

6.2.1 The IS auditor should study and evaluate the following during the course of the review to assess the risks/issues and their effects. While some of these are relevant for all the SDLC reviews, irrespective of the type of review (pre-implementation, parallel/concurrent or post-implementation), some are relevant for specific types of review alone. The IS auditor should study and evaluate those aspects that are relevant for the objectives and scope of the proposed review, so as to arrive at the appropriate assessment of the risks and issues as well as the recommendations to mitigate their effects, such as:
- Project charter (including the project plan, deliverables and their schedules) and business case (highlighting costs and benefits) for the application system
- Project structure including any working groups, steering groups, and the related roles and responsibilities
- The formal project management methodology adopted, if any (such as PRINCE 2), and the related process of creating the customised design of processes
- The development or application development methodology, such as waterfall development, prototyping, rapid application development, CASE, and object-oriented development, and the associated tools chosen for the application system
- Contracts with suppliers for purchased application systems
- Contracts with suppliers for outsourced services, such as customisation and/or development
- Control processes within the SDLC model—particularly reviews, validations, approvals and sign-offs for the SDLC stages under review
- Structure of the deliverables for the SDLC stages under review
- Minutes of relevant meetings, such as working group and steering group meetings
- Actual deliverables, as well as the audit trails of their reviews and sign-off
- Project reporting, progress tracking (efforts, time and cost) and escalation
- Resource management
- Ongoing risk management
- Quality management/assurance
- Change management
- Performance and problem management including service level agreements (SLAs)
- Configuration management
- Data conversion/migration
- Documentation relating to in-project reviews including testing
- In-project and supplier communications
- Reviews, if any, of earlier SDLC stages of the application system
- Earlier SDLC reviews, if any, of similar applications
- Relevant legal, regulatory and policy aspects to be complied with, if any

6.2.2 CoeIT defines the high-level control objectives with reference to acquisition of application systems, which includes areas such as Identify Automated Solutions (A11) and Acquire and Maintain Application Software (A12). Similarly, there are high-level control objectives regarding Manage Projects (PO10), Manage Quality (PO11) and Ensure System Security (DS5). Within CoeIT, these are further expanded into detailed control objectives. As part of the review, the IS auditor should evaluate the extent to which these control objectives (relevant to the SDLC stages under review) are met and the effectiveness of the mechanisms and procedures employed to achieve such objectives.

6.2.3 CoeIT also defines seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability) to be met by application systems. As part of the review of the SDLC of an application system, the IS auditor also should evaluate how effectively the SDLC processes/stages under review contribute towards the adequate fulfilment of these criteria. Actual evaluation of the compliance of the application system with these criteria would be part of the application system review (refer to guideline G14 Application Systems Review).

7. REPORTING

7.1 IS Auditor’s Report

7.1.1 For SDLC reviews of application systems, often, reporting could be performed progressively, as and when risks and issues are identified. These reports should be addressed to the appropriate management for necessary action. A final report listing all issues raised during the review can be issued.

7.1.2 Depending on the type of review, the report should address aspects, such as:
- Appropriateness of the SDLC model and development methodology
8. **FOLLOW-UP**

8.1 **Timely Follow-up**

8.1.1 For SDLC reviews of application systems, particularly, the pre-implementation and parallel/concurrent reviews, there should be an appropriate follow-up to provide reasonable assurance that the risk mitigation actions are taken in a timely manner. In the case of post-implementation reviews, the follow-up should focus on the timeliness of corrective actions in the downstream stages and in similar future projects.

9. **EFFECTIVE DATE**

9.1 This guideline is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.htm.

**APPENDIX**

**CobiT Reference**

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 information criteria.

In the case of this specific audit area, review of the SDLC, the processes in CobiT likely to be the most relevant are: selected Planning and Organising IT processes, all the Acquire and Implement IT processes, and selected Delivery and Support. Therefore, CobiT guidance for the following processes should be considered relevant when performing the audit:

- PO8—Ensure Compliance with External Requirements
- PO10—Manage Projects
- PO11—Manage Quality
- AI1—Identify Automated Solutions
- AI2—Acquire and Maintain Application Software
- AI3—Acquire and Maintain Technology Infrastructure
- AI4—Develop and Maintain Procedures
- AI5—Install and Accredit Systems
- AI6—Manage Changes
- DS1—Define and Manage Service Levels
- DS2—Manage Third-party Services
- DS3—Manage Performance and Capacity
- DS4—Ensure Continuous Service
- DS5—Ensure Systems Security
- DS7—Educate and Train Users

The information criteria most relevant to an SDLC audit are:

- Primary: effectiveness and efficiency
- Secondary: confidentiality, integrity, availability, compliance and reliability

© Copyright 2003
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1546
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web Site: www.isaca.org