Information Systems Audit and Control Association

IS AUDITING GUIDELINE
FOLLOW-UP ACTIVITIES
DOCUMENT G35

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 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.

COBIT® resources should be used as a source of best practice guidance. 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". 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 information criteria.

As defined in the COBIT framework*,* each of the following is organised by IT management process. COBIT is intended for use by business and IT management as well as IS auditors; therefore, its usage enables the understanding of business objectives, communication of best practices, and recommendations to be made around a commonly understood and well-respected standard reference. COBIT includes:

- 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. They 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? 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.
  - 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? 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.

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 on 1 December 2005.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S8 Follow-up Activities states, "After the reporting of findings and recommendations, the IS auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner".

1.2 Linkage to CobiT

1.2.1 High-level control objective M3 (*Obtain independent assurance*) states, "…obtaining independent assurance to increase confidence and trust amongst the organisations, customers and third-party providers".

1.2.2 High-level control objective M4 (*Provide for independent audit*) states, "…providing for independent audit to increase confidence levels and benefit from best practice advice".

1.2.3 Detailed control objective M4.8 (*Follow-up activities*) states, "Resolution of audit comments rests with management. Auditors should request and evaluate appropriate information on previous findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner".

1.3 CobiT Reference

1.3.1 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 requirement, the processes in CobiT likely to be the most relevant selected and adapted are classified below as primary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- M3—*Obtain independent assurance*
- M4—*Provide for independent audit*

1.3.3 The information criteria most relevant to competence are:

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

1.4 Purpose of the Guideline

1.4.1 The purpose of this guideline is to provide direction to IS auditors engaged in following up on recommendations and audit comments made in reports.

1.4.2 This guideline provides guidance in applying IS Auditing Standard S8 Follow-up Activities.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

2. FOLLOW-UP ACTIVITIES

2.1 Definition

2.1.1 Follow-up activities by IS auditors can be defined "as a process by which they determine the adequacy, effectiveness and timeliness of actions taken by management on reported engagement observations and recommendations, including those made by external auditors and others".[1]

2.1.2 A follow-up process should be established to help provide reasonable assurance that each review conducted by the IS auditors provides optimal benefit to the organisation by requiring that agreed-upon outcomes arising from reviews are implemented in accordance with management undertakings or that management recognises and acknowledges the risks inherent in delaying or not implementing proposed outcomes.

2.2 Management's Proposed Actions

2.2.1 As part of the IS auditor's discussions with the engagement organisation, the IS auditor should obtain agreement on the results of the engagement and on a plan of action to improve operations, as needed.

2.2.2 Management should provide an implementation/action date when each proposed action is to be completed.

2.2.3 When management's proposed actions to implement or otherwise address reported recommendations and audit comments have been discussed with or provided to the IS auditor, these actions should be recorded as a management response in the final report with a committed implementation date.

2.2.4 If the IS auditor and engagement organisation disagree about a particular recommendation or audit comment, the engagement communications may state both positions and the reasons for the disagreement. The organisation's written comments may be included as an appendix to the engagement report. Alternatively, the organisation's views may be presented in the body of the report or in a cover letter. Senior management (or the audit committee if one exists) should then make a decision as to which point of view they support. If senior management (or the audit committee) supports the view of the organisation in a particular case, the IS auditor need not follow-up with that particular recommendation, unless it is considered that the significance and level of effect of the observation has changed due to a change(s) in the IS environment (refer to section 2.4.3).

[1] Institute of Internal Auditors (IIA), "Practice Advisory 2500.A1-1," 2002

2.2.5 During some reviews, such as pre-implementation application system reviews, findings may be reported to the project team and/or management on an ongoing basis often in the form of issue statements. In these cases, actions to resolve issues raised should be monitored on an ongoing basis. If issue statement recommendations have been implemented, then "completed" or "implemented" can be recorded against the recommendation in the final report. "Completed" or "implemented" recommendations should be reported.

2.3 Follow-up Procedures

2.3.1 Procedures for follow-up activities should be established and should include:

- The recording of a time frame within which management should respond to agreed-upon recommendations
- An evaluation of management's response
- A verification of the response, if thought appropriate (refer to section 2.7)
- Follow-up work, if thought appropriate
- A communications procedure that escalates outstanding and unsatisfactory responses/actions to the appropriate levels of management
- A process for providing reasonable assurance of management's assumption of associated risks, in the event that remedial action is delayed or not proposed to be implemented

2.3.2 An automated tracking system or database can assist in the carrying out of follow-up activities.

2.3.3 Factors that should be considered in determining appropriate follow-up procedures are:

- Any changes in the IS environment that may affect the significance of a reported observation
- The significance of the reported finding or recommendation
- The effect that may result should the corrective action fail
- The degree of effort and cost needed to correct the reported issue
- The complexity of the corrective action
- The time period involved

2.3.4 If the IS auditor is working in an internal audit environment, responsibility for follow-up should be defined in the internal audit activity's written charter.

2.4 Timing and Scheduling of Follow-up Activities

2.4.1 The nature, timing and extent of the follow-up activities should take into account the significance of the reported finding and the effect if corrective action is not taken. The timing of IS audit follow-up activities in relation to the original reporting is a matter of professional judgement dependent on a number of considerations, such as the nature or magnitude of associated risks and costs to the organisation.

2.4.2 Agreed-upon outcomes relating to high-risk issues should be followed up soon after the due date for action and may be monitored progressively.

2.4.3 Because they are an integral part of the IS audit process, follow-up activities should be scheduled, along with the other steps necessary to perform each review. Specific follow-up activities and the timing of such activities may be influenced by the results of the review and may be established in consultation with line management.

2.4.4 In a particular report, the implementation of all the management responses may be followed up together even though the implementation dates committed to by management may be different. Another approach is to follow up individual management responses according to the due date agreed to with management.

2.5 Deferring Follow-up Activities

2.5.1 The IS auditor is responsible for scheduling follow-up activities as part of developing engagement work schedules. The scheduling of follow-ups should be based on the risk and exposure involved, as well as the degree of difficulty and the significance of timing in implementing corrective action.

2.5.2 There may also be instances where the IS auditor judges that management's oral or written response shows that action already taken is sufficient when weighed against the relative importance of the engagement observation or recommendation. On such occasions, actual follow-up verification activities may be performed as part of the next engagement that deals with the relevant system or issue.

2.6 The Form of Follow-up Responses

2.6.1 The most effective way to receive follow-up responses from management is in writing, as this helps to reinforce and confirm management responsibility for follow-up action and progress achieved. Also, written responses ensure an accurate record of actions, responsibilities and current status. Oral responses may also be received and recorded by the IS auditor and where possible approved by management. Proof of action or implementation of recommendations may also be provided with the response.

2.6.2 The IS auditor may request and/or receive periodic updates from management to evaluate the progress management has made to carry out its agreed-upon actions, particularly in relation to high-risk issues and remedial actions with long lead times.

2.7 Nature and Extent of Follow-up Activities

2.7.1 Normally, the IS auditor will request follow-up status from the organisation soon after the proposed implementation date of some or all of the agreed-upon actions has passed. This may involve reformatting the final report to give the organisation an area in the report to document the details of actions taken to implement recommendations.

2.7.2 The organisation will normally be given a time frame within which to respond with details of actions taken to implement recommendations.

2.7.3 Management's response detailing the actions taken should be evaluated, if possible, by the IS auditor who performed the original review. Wherever possible, audit evidence of action taken should be obtained. For example, procedures may have been documented or a certain management report produced.

2.7.4 Where management provides information on actions taken to implement recommendations and the IS auditor has doubts about the information provided or the effectiveness of the action taken, appropriate testing or other audit procedures should be undertaken to confirm the true position or status prior to concluding follow-up activities.

2.7.5 As a part of the follow-up activities, the IS auditor should evaluate whether unimplemented findings are still relevant or have a greater significance. The IS auditor may decide that the implementation of a particular recommendation is no longer appropriate. This could occur where application systems have changed, where compensating controls have been implemented, or where business objectives or priorities have changed in such a way as to effectively remove or significantly reduce the original risk. In the same way, a change in the IS environment may increase the significance of the effect of a previous observation and the need for its resolution.

2.7.6 A follow-up engagement may have to be scheduled to verify the implementation of critical/important actions.

2.7.7 The IS auditor's opinion on unsatisfactory management responses or action should be communicated to the appropriate level of management.

2.8 Acceptance of Risks by Management

2.8.1 Management is responsible for deciding the appropriate action to be taken in response to reported engagement observations and recommendations. The IS auditor is responsible for assessing such management action for appropriateness and the timely resolution of the matters reported as engagement observations and recommendations.

2.8.2 Senior management may decide to accept the risk of not correcting the reported condition because of cost or other considerations. The board (or the audit committee if one exists) should be informed of senior management's decision on all significant engagement observations and recommendations.

2.8.3 When the IS auditor believes that the organisation has accepted a level of residual risk that is inappropriate for the organisation, the IS auditor should discuss the matter with internal audit and senior management. If the IS auditor is not in agreement with the decision regarding residual risk, the IS auditor and senior management should report the matter to the board (or the audit committee, if one exists) for resolution.

2.9 External Audit Follow-up by an Internal IS Auditor

2.9.1 Follow-up responsibilities for ongoing internal audit activities should be assigned in the audit charter of the internal IS audit function, and for other audit assignments in the engagement letters.

2.9.2 Depending on the scope and terms of the engagement and in accordance with the relevant IS Auditing Standards, external IS auditors may rely on an internal IS audit function to follow-up on their agreed-upon recommendations.

3. CONSULTING

3.1 Consulting Type Engagements

3.1.1 Consulting type engagements or services can be defined as "advisory and related client service activities, the nature and scope of which are agreed upon with the client and which are intended to add value and improve an organisation's operations. Examples include counsel, advice, facilitation, process design and training."[2] The nature and scope of the engagement should be agreed before the engagement begins.

3.1.2 The IS auditor should monitor the results of consulting engagements to the extent agreed upon with the organisation. Varying types of monitoring may be appropriate for differing types of consulting engagements. The monitoring effort may depend on factors, such as, management's explicit interest in the engagement outcomes or the IS auditor's assessment of the project's risks and/or potential additional value to the organisation identified by the engagement.

4. REPORTING

4.1 Reporting of Follow-up Activities

4.1.1 A report on the status of agreed remedial actions arising from IS audit reports, including agreed recommendations not implemented, should be presented to the audit committee, if one has been established, or alternatively to the appropriate level of organisation management.

4.1.2 If during a subsequent engagement, the IS auditor finds that the action that management had purported as "implemented" had in fact not been implemented, this should be communicated to senior management and the audit committee if one is in place.

4.1.3 When all the agreed remedial actions have been implemented, a report detailing all the implemented/completed actions can be forwarded to senior management (or the audit committee, if one exists).

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning 1 March 2006. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

[2] International Standards for the Professional Practice of Internal Auditing, Glossary, IIA

Information Systems Audit and Control Association
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*