IS Audit and Assurance Guideline 2402 Follow-up Activities

The specialised nature of information systems (IS) audit and assurance and the skills necessary to perform such engagements require standards that apply specifically to IS audit and assurance. The development and dissemination of the IS audit and assurance standards are a cornerstone of the ISACA® professional contribution to the audit community.

IS audit and assurance standards define mandatory requirements for IS auditing and reporting and inform:

- IS audit and assurance professionals 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 committee and, ultimately, in disciplinary action.

IS audit and assurance professionals should include a statement in their work, where appropriate, acknowledging that the engagement has been conducted in accordance with ISACA IS audit and assurance standards or other applicable professional standards.

ITAF™, a professional practices framework for IS audit and assurance, provides multiple levels of guidance:

- **Standards**, divided into three categories:
  - General standards (1000 series)—Are the guiding principles under which the IS audit and assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill. The standards statements (in **bold**) are mandatory.
  - Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care
  - Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated
- **Guidelines**, supporting the standards and also divided into three categories:
  - General guidelines (2000 series)
  - Performance guidelines (2200 series)
  - Reporting guidelines (2400 series)
- **Tools and techniques**, providing additional guidance for IS audit and assurance professionals, e.g., white papers, IS audit/assurance programmes, the COBIT® 5 family of products

An online glossary of terms used in ITAF is provided at *www.isaca.org/glossary*.

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, controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IS environment.

The ISACA Professional Standards and Career Management Committee (PSCMC) is committed to wide consultation in the preparation of standards and guidance. Prior to issuing any document, an exposure draft is issued internationally for general public comment. Comments may also be submitted to the attention of the director of professional standards development via email (*standards@isaca.org*), fax (+1.847. 253.1443) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

The guideline is presented in the following sections:
1. Guideline purpose and linkage to standards
2. Guideline content
3. Linkage to standards and COBIT 5 processes
4. Terminology
5. Effective date

1. Guideline Purpose and Linkage to Standards

1.0 Introduction

This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose

1.1.1 The purpose of this guideline is to provide guidance to IS audit and assurance professionals in monitoring if management has taken appropriate and timely action on reported recommendations and audit findings.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards

1.2.1 Standard 1401 Reporting
1.2.2 Standard 1402 Follow-up Activities

1.3Term Usage

1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Follow-up process
2.2 Management's proposed actions
2.3 Assuming the risk of not taking corrective action
2.4 Follow-up procedures
2.5 Timing and scheduling of follow-up activities
2.6 Nature and extent of follow-up activities
2.7 Deferring follow-up activities
2.8 Form of follow-up responses
2.9 Follow-up by professionals on external audit recommendations
2.10 Reporting of follow-up activities

2.1 Follow-up Process

2.1.1 Follow-up activity performed by professionals is a process by which they determine the adequacy, effectiveness and timeliness of actions taken by management on reported observations and recommendations, including those made by external auditors and others.

2.1.2 A follow-up process should be established to help provide reasonable assurance that each review conducted by professionals provides optimal benefit to the enterprise by requiring that agreed-on outcomes arising from reviews are implemented in accordance with management undertakings or that (executive) management recognises and acknowledges the risk of delaying or not implementing proposed outcomes and/or recommendations.

2.2 Management's Proposed Actions

2.2.1 As part of their discussions with the auditee, professionals should obtain agreement on the results of the audit engagement and on a plan of action to improve operations, as needed.

2.2.2 Professionals should discuss with management the proposed actions to implement or address reported recommendations and audit comments. These proposed actions should be provided to professionals and should be recorded as a management response in the final report with a committed implementation and/or action date.

2.2.3 If professionals and the auditee come to an agreement on the proposed actions, professionals should initiate the procedures for follow-up activities, as detailed in section 2.4.

2.3 Assuming the Risk of Not Taking Corrective Action

2.3.1 (Executive) management may decide to accept the risk of not correcting the reported condition because of cost, complexity of the corrective action or other considerations. The board (or those charged with governance) should be informed of (executive) management's decision on all significant engagement observations and recommendations for which management accepts the risk of not correcting the reported situation.

2.3.2 When professionals believe that the auditee has accepted a level of residual risk that is inappropriate for the enterprise, they should discuss the matter with IS audit and assurance management and executive management. If professionals remain in disagreement with the decision regarding residual risk, they, along with executive management, should report the matter to the board (or those charged with governance) for resolution.

2.3.3 Acceptance of risk should be documented and formally approved by executive management and communicated to those charged with governance.

2.4 Follow-up Procedures

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

- The recording of a time frame within which management should respond to agreed-on recommendations
- An evaluation of management's response
- A verification of the response, if appropriate (refer to section 2.6)
- Follow-up work, if appropriate
- A communication procedure that escalates outstanding and unsatisfactory responses and/or actions to the appropriate levels of management and to those charged with governance
- A process for obtaining management's assumption of associated risk, in the event that corrective action is delayed or not proposed to be implemented

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

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

- The importance and impact of the findings and recommendations
- Any changes in the IS environment that may affect the importance and impact of the findings and recommendations
- The complexity of correcting the reported situation
- The time, cost and effort needed to correct the reported situation
- The effect if correcting the reported situation should fail

2.4.4 Responsibility for follow-up actions, reporting and escalation should be defined in the audit charter.

2.5 Timing and Scheduling of Follow-up Activities

2.5.1 The timing of the follow-up activities should take into account the significance of the reported findings and the effect if corrective actions are not taken. The timing of 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 risk and costs to the enterprise.

2.5.2 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 degree of difficulty, the risk and exposure involved, the results of the review, the time needed for implementing corrective actions, etc., and may be established in consultation with management.

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

2.5.4 The implementation of all the management responses may be followed up on a regular basis (e.g., each quarter) for different audit engagements 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 on with management.

2.6 Nature and Extent of Follow-up Activities

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

2.6.2 Management's response detailing the actions taken should be evaluated, if possible, by professionals who performed the original review. Wherever possible, audit evidence of action taken should be obtained.

2.6.3 Where management provides information on actions taken to implement recommendations and professionals have 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 further follow-up activities.

2.6.4 As a part of the follow-up activities, professionals should evaluate whether unimplemented recommendations are still relevant or have a greater significance. Professionals 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.

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

2.6.6 Professionals' opinion on unsatisfactory management responses or action should be communicated to the appropriate level of management.

2.7 Deferring Follow-up Activities

2.7.1 Professionals are 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 time needed in implementing corrective actions.

2.7.2 There may also be instances where professionals judge 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.

2.8 Form of Follow-up Responses

2.8.1 The most effective way to receive follow-up responses from management is in writing, because 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 professionals and, where possible, approved by management. Proof of action or implementation of recommendations may also be provided with the response.

2.8.2 Professionals should request and/or receive periodic updates from management responsible for implementing agreed-on actions to evaluate the progress management has made, particularly in relation to high-risk issues and corrective actions with long lead times.

2.9 Follow-up by Professionals on External Audit Recommendations

2.9.1 Depending on the scope and terms of the audit engagement and in accordance with the relevant IS auditing standards, external professionals may rely on internal professionals to follow-up on their agreed-on recommendations. Responsibilities regarding this follow-up can be determined in the audit charter or engagement letters.

2.10 Reporting of Follow-up Activities

2.10.1 A report on the status of agreed-on corrective actions arising from audit engagement reports, including agreed-on recommendations not implemented, should be presented to the appropriate level of management and to those charged with governance (e.g., the audit committee).

2.10.2 If, during a subsequent audit engagement, professionals find that the corrective action that management had reported as 'implemented' had in fact not been implemented, they should communicate this to the appropriate level of management and those charged with governance. If appropriate, the professional should obtain a current corrective action plan and planned implementation date.

2.10.3 When all the agreed-on corrective actions have been implemented, a report detailing all the implemented and/or completed actions can be forwarded to executive management and those charged with governance.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:

3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:

- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1401 Reporting	IS audit and assurance professionals shall provide a report to communicate the results upon completion of the engagement including: • Identification of the enterprise, the intended recipients and any restrictions on content and circulation • The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed • The findings, conclusions, and recommendations

Standard Title	Relevant Standard Statements
	• Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement • Signature, date and distribution according to the terms of the audit charter or engagement letter IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient, reliable and relevant evidence.
1402 Follow-up Activities	IS audit and assurance professionals shall monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
- COBIT 5 processes
- COBIT 5 process purpose.

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes*.

COBIT 5 Process	Process Purpose
EDM01 Ensure governance framework setting and maintenance.	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.
EDM02 Ensure benefits delivery.	Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
EDM03 Ensure risk optimisation.	Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:

- Colleagues from within the enterprise
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Follow-up activity	A process by which internal auditors evaluate the adequacy, effectiveness, and timeliness of actions taken by management on reported observations and recommendations, including those made by external auditors and others. Source: Institute of Internal Auditors—Practice Advisory 2500.A1-1; Copyright © by The Institute of Internal Auditors, Inc. All rights reserved.
Professional judgement	The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.