IT AUDIT AND ASSURANCE GUIDELINE

G42 CONTINUOUS ASSURANCE

The specialised nature of information technology (IT) audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards is a cornerstone of the ISACA professional contribution to the audit and assurance community. There are multiple levels of guidance:

- **Standards** define mandatory requirements for IT audit and assurance. They inform:
  - IT 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 ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional 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 IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow. The tools and techniques documents provide information on how to meet the standards when performing IT audit and assurance work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

COBIT® 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 enterprises. It emphasises regulatory compliance, helps enterprises 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 IT audit and assurance professionals; 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 IT Audit and Assurance Standards, Guidelines, and Tools and Techniques.

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 Professional Standards Committee is committed to wide consultation in the preparation of the IT Audit and Assurance Standards, Guidelines, and Tools and Techniques. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Professional Standards Committee 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 Val IT initiative manager. This material was issued on 1 March 2010.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning states that the IT audit and assurance professional should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards.

1.1.2 Standard S6 Performance of Audit Work states that during the course of the audit, the IT audit and assurance professional should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by the appropriate analysis and interpretation of this evidence.

1.1.3 Standard S7 Reporting states that the IT audit and assurance professional should have sufficient and appropriate audit evidence to support the results reported.

1.1.4 Standard S14 Audit Evidence states that the IT audit and assurance professional should obtain sufficient and appropriate audit evidence to draw reasonable conclusions on which to base the audit results.

1.2 Linkage to Guidelines

1.2.1 Guideline G2 Audit Evidence Requirement provides guidance to the IT audit and assurance professional regarding the type and sufficiency of audit evidence used in information systems auditing.

1.2.2 Guideline G3 Use of Computer-assisted Audit Techniques (CAATs) provides guidance to the IT audit and assurance professional regarding the use of the many types of computer-assisted tools and techniques that can be used in performing various audit procedures.

1.2.3 Guideline G10 Audit Sampling provides guidance to the IT audit and assurance professional regarding the design and selection of an audit sample and evaluation of sample results.

1.3 Linkage to COBIT

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 IT governance requirement of IT audit and assurance professionals, the processes in COBIT most likely to be relevant, selected and adapted are classified here 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 The primary references are:

- DS5 *Ensure systems security*
- ME2 *Monitor and evaluate internal control*
- AI1 *Identify automated solution*

1.3.3 The information criteria most relevant are:

- Primary: Effectiveness, efficiency, confidentiality and integrity
- Secondary: Availability, compliance and reliability

1.4 Need for Guideline

1.4.1 Traditionally, the testing of controls has been performed on a retrospective and cyclical basis, often many months after business activities have occurred. The testing procedures have often been based on a sampling approach and included activities such as reviews of policies, procedures, approvals and reconciliations. Continuous assurance is a method used to perform control and risk assessments automatically on a more frequent basis. The main benefit of this approach is the intelligent and efficient continuous testing of controls and risks that result in timely notification of gaps and weaknesses to allow immediate follow-up and remediation.

1.4.2 While continuous assurance as a concept is not strictly limited to IT audit, IT audit and assurance professionals are often called upon to develop, implement and maintain continuous assurance processes and systems for their clients or within their enterprises. IT audit and assurance professionals can add value by leveraging the unique combination of business and technical skills and experience necessary to successfully implement continuous assurance processes and systems and engage the broad range of business and IT stakeholders involved.

1.4.3 This guideline provides guidance to IT audit and assurance professionals in applying the relevant IT audit and assurance standards during the planning, implementation and maintenance of continuous assurance processes and systems within an enterprise.

2. CONTINUOUS ASSURANCE, AUDITING AND MONITORING

2.1 CAATs and Continuous Assurance

2.1.1 Computer-assisted audit techniques (CAATs) are any automated audit technique that relate to generalised audit software, test data generators, integrated test facilities, computerized audit programs, and specialised audit and system software utilities.

2.1.2 Continuous assurance is an uninterrupted monitoring approach. It is a combination of an IT audit and assurance professional's oversight of management's continuous monitoring and an IT audit and assurance professional's continuous auditing approach using CAATs that allows management and IT audit and assurance professionals to monitor controls and risk on a continuous basis and to gather selective audit evidence using technology.

2.1.3 Continuous assurance is a process that can be used to provide timely reporting by IT audit and assurance professionals and lends itself to use in high-risk, high-volume paperless environments. It is an important tool for the IT audit and assurance professional to evaluate the control environment in an efficient and effective manner, and leads to increased audit coverage, more thorough and consistent analysis of data, and reduction in risk.

2.2 Continuous Auditing

2.2.1 Continuous auditing is a method used by the IT audit and assurance professional to perform control and risk assessments on a more frequent basis. It is a method using CAATs that allows IT audit and assurance professionals to monitor controls and risk on a continuous basis. This approach allows the IT audit and assurance professional to gather selective audit evidence through the computer.

2.3 Continuous Monitoring

2.3.1 Continuous monitoring is a management process to monitor whether policies, procedures and business processes are operating effectively on an ongoing basis. In addition to management-developed continuous monitoring processes, continuous auditing performed by IT audit and assurance professionals, when appropriate, may be transitioned to management, in which case it becomes a continuous monitoring procedure performed by management. Management's use of continuous monitoring procedures in conjunction with continuous auditing performed by the IT audit and assurance professional will satisfy the demands for assurance that control procedures are effective and that information produced for decision making is relevant and reliable.

3. PLANNING

3.1 Choosing Areas for Continuous Audit

3.1.1 The activity of choosing which areas to review using continuous auditing should be integrated as part of the development of the annual audit plan and should utilise the enterprise's risk management framework, if one has been developed. Rather than scheduling reviews according to a standard cycle, the frequency of reviews should be based on the risk factors in an area or business process. The IT audit and assurance professional should consider the following when deciding priority areas for continuous auditing:

- Identify the critical business processes that should be reviewed and prioritised based on risk.
- Review the enterprise's risk management framework, if one has been developed.
- Consider prior experience reviewing areas of the enterprise.
- Ascertain the availability and integrity of continuous auditing data for the risk areas identified.
- Prioritise the identified areas for review, considering where timely reporting of results might be of greater value to the enterprise.
- Determine the review frequency of the areas under review.
- Set the audit objectives of the areas to be reviewed that may be included in the terms of reference for the exercise.

4. RISK MANAGEMENT

4.1 Risk Identification and Assessment

4.1.1 Continuous auditing helps IT audit and assurance professionals to identify and assess risk and establish intelligent and dynamic thresholds that respond to changes in the enterprise. It also

supports risk identification and assessment for the entire audit universe, contributing to the development of the annual audit plan as well as the objectives of a specific audit. The IT audit and assurance professional should review the enterprise's risk management framework, if one has been developed.

5. IMPLEMENTATION OF CONTINUOUS AUDITING

5.1 Engagement Planning

5.1.1 Successful implementation of continuous auditing requires the buy-in of stakeholders, including management, and a phased approach that initially addresses the most critical business systems. The following activities must be planned and managed when developing and supporting the use of continuous auditing:

- Prioritise areas for coverage and select an appropriate continuous auditing approach.
- Ensure the availability of key client personnel.
- Select the appropriate analysis tool—this could be in-house written routines or vendor-provided software.
- Develop continuous auditing routines to assess controls and identify deficiencies.
- Determine the frequency of applying continuous auditing routines.
- Define output requirements.
- Develop a reporting process.
- Establish relationships with relevant line and IT management.
- Assess data integrity and prepare data.
- Determine resource requirements, i.e., personnel, processing environment (the enterprise's IT facilities or IT audit facilities).
- Understand the extent to which management is performing its monitoring role (continuous monitoring).

5.2 Obtaining Management Support

5.2.1 Once the objectives of continuous auditing have been defined, senior management support should be obtained. Senior management must be informed of the preconditions, in particular the access requirements, as well as how and when the results will be reported. If this is done, when anomalies in transactions are identified and managers are contacted for explanations, the legitimacy of the continuous auditing activity will not be questioned.

5.2.2 Support from management can be obtained in conjunction with the approval of the terms of reference for the continuous auditing coverage. Support also should be obtained from the audit committee, if one has been formed. The period covered by the terms of reference for continuous auditing is usually longer than the period covered for a single assignment, and it is not unusual for the period covered to be up to one year.

5.3 Arrangements With the Auditee

5.3.1 Data files, such as detailed transaction files, are often only retained for a short period of time. Therefore, the IT audit and assurance professional should make arrangements for the retention of the data to cover the appropriate audit time frame.

5.3.2 Access to the enterprise's IT facilities, programs/system and data should be arranged well in advance of the needed time period to minimise the effect on the enterprise's production environment.

5.3.3 The IT audit and assurance professional should assess the effect that changes to the production programs/system may have on the use of continuous auditing routines. In doing so, the IT audit and assurance professional should consider the effect of these changes on the integrity and usefulness of the continuous auditing routines as well as the integrity of the programs/system and data used by the IT audit and assurance professional.

5.4 Developing Continuous Auditing Routines

5.4.1 The IT audit and assurance professional should obtain reasonable assurance of the integrity, reliability, usefulness and security of the continuous auditing routines, through appropriate planning, design, testing, processing and review of documentation. This should be done before reliance is placed on the continuous auditing routines. The IT audit and assurance professional should be able to demonstrate that the system development life cycle has been followed to ensure completeness and accuracy of the continuous auditing routines.

5.5 Scope of Continuous Assurance Testing

5.5.1 The extent to which detailed testing of controls and risks must be performed by the IT audit and assurance professional needs to be determined. A key factor in this determination will be the adequacy of the control environment and monitoring activities. The IT audit and assurance professional should examine the control framework and areas addressed by the enterprise risk management framework, if one has been developed. If management has well-established and functioning processes, including continuous monitoring, to assess controls and risk, the IT audit and assurance professional will be able to place more reliance on the control and risk levels being reported. However, if the processes are not adequate, the IT audit and assurance professional will, out of necessity, be required to perform detailed assessments of the controls and risks on a more continual basis.

5.6 Frequency of Testing

5.6.1 The IT audit and assurance professional should consider the objectives of continuous auditing, the risk appetite of the enterprise, the level and nature of management's continuous monitoring, and the enterprise risk activities, when setting the timing, scope and coverage of continuous auditing tests. IT audit and assurance professionals should prioritise the risks and select only a few high-risk areas or key control points for the first implementation of continuous auditing.

5.6.2 The next step is determining how often the continuous auditing tests will be run. The frequency of continuous auditing activities will range from a real-time or near real-time review of detailed transactions, to periodic analysis of detailed transactions, snapshots or summarised data. The frequency will depend not only on the level of risk associated with the system or process being examined, but also on the adequacy of the monitoring performed by management and resources available. Critical systems with key controls may be subject to real-time analysis of transactional data. Risk assessments to support the annual audit plan may be conducted quarterly, while those supporting individual auditing and the tracking of audit recommendations may occur on an *ad hoc* basis. The frequency of running continuous auditing routines should depend on risk. An important consideration when discussing frequency is that the automation of continuous auditing tests will lower the cost of performing risk assessments and control verification.

5.6.3 Finally, when determining how often and where continuous auditing will be performed, the IT audit and assurance professional should consider not only the regulatory requirements, but also the degree to which management is addressing the risk exposures and potential impacts. When management has implemented continuous monitoring systems for controls, internal and external audit and assurance professionals can take this into account and decide the extent to which they can rely on the continuous monitoring processes to reduce detailed controls testing.

5.7 Data Integrity and Security Concerns

5.7.1 Where continuous auditing routines are used to extract information for data analysis, the IT audit and assurance professional should verify the integrity of the information systems and IT environment from which the data have been extracted.

5.7.2 Sensitive program/system information and production data should be kept securely. The IT audit and assurance professional should safeguard the program/system information and production data with an appropriate level of security to ensure confidentiality. In doing so, the IT audit and assurance professional should consider the level of confidentiality and security required by the enterprise owning the data and any relevant legislation.

5.7.3 The IT audit and assurance professional should use and document the results of appropriate procedures to provide for the ongoing integrity, reliability, usefulness and security of the continuous auditing routines. For example, this should include a review of program maintenance and program change controls to determine that only authorised changes were made to the continuous auditing routines.

5.7.4 When the continuous auditing routines reside in an environment not under the control of the IT audit and assurance professional, an appropriate level of control should be in effect to identify changes to the continuous auditing routines. When the continuous auditing routines are changed, the IT audit and assurance professional should obtain assurances of their integrity, reliability, usefulness and security, through appropriate planning, design, testing, processing and review of documentation, before reliance is placed on the continuous auditing routines.

6. OVERSIGHT OF CONTINUOUS MONITORING

6.1 Continuous Monitoring

6.1.1 Continuous monitoring refers to the processes that management puts in place to ensure that the policies, procedures and business processes are operating effectively. It typically addresses management's responsibility to assess the adequacy and effectiveness of controls. Many of the techniques management uses to continuously monitor controls are similar to those that may be performed in continuous auditing by the IT audit and assurance professional. Continuous assurance also monitors the effectiveness of management monitoring.

6.1.2 The key to continuous monitoring is that the process should be owned and performed by management as part of its responsibility to implement and maintain an effective control environment. Since management is responsible for internal controls, it should have a means to determine, on an ongoing basis, whether the controls are operating as designed. By being able to identify and correct control problems on a timely basis, the overall control system can be improved. A typical additional benefit to the enterprise is that instances of error and fraud can be reduced. There is an inverse relationship between the adequacy of management's monitoring and risk management activities and the extent to which IT audit and assurance professionals must perform detailed testing of controls and assessments of risk. The IT audit and assurance professional's approach to, and amount of, continuous auditing depends on the extent to which management has implemented continuous monitoring.

6.2 Responsibilities of Management

6.2.1 Management is responsible for implementing processes and systems that continuously monitor the control environment to ensure that the operation of key controls, including policies, procedures and business processes, is meeting the intended business objectives in an efficient and effective manner.

6.2.2 Management may use various techniques to implement continuous monitoring of the control environment, including:

- Defining the risk and control points within a business process
- Identifying the control objectives and assertions for the business process
- Designing manual and automated controls to address the specific control objectives
- Testing the operation of these manual and automated controls
- Monitoring the operation of the manual and automated controls across normal business transactions
- Investigating control exceptions identified by management controls
- Taking any necessary action to remedy control weaknesses or transaction errors detected
- Updating and retest manual and automated controls to reflect changing business processes

6.3 Responsibilities of IT Audit and Assurance Professionals

6.3.1 IT audit and assurance professionals are required to provide oversight and assurance to the audit committee, if one has been formed, and other key stakeholders that continuous monitoring processes and systems are operating in an efficient and effective manner to address specific control objectives.

6.3.2 IT audit and assurance professionals may use several techniques to oversee the operation of management's continuous monitoring activities, including:

- Reviewing and testing the controls over the development of continuous monitoring mechanisms, including the documentation, systems development life cycle, training, logical access and change controls relating to key continuous monitoring activities
- Comparing the output of management's continuous monitoring activities to the results of similar continuous auditing procedures executed by the IT audit and assurance professional, for instance, comparing exception reports to ensure that the management reports are detecting potential errors completely and accurately
- Reviewing prior management reports and discussing with management what actions have been taken on the exceptions noted and the outcomes of such actions

7. PERFORMANCE OF CONTINUOUS AUDITING WORK

7.1 Gathering Audit Evidence

7.1.1 The use of continuous auditing routines should be controlled by the IT audit and assurance professional to provide reasonable assurance that the audit objectives and the detailed specifications of the routines have been met. The IT audit and assurance professional should:

- Perform a reconciliation of control totals where appropriate
- Review output for reasonableness
- Perform a review of the logic, parameters or other characteristics of the routines
- Review the enterprise's general IT controls that may contribute to the integrity of the continuous auditing routines (e.g., program change controls and access to system, program, and/or data files)

7.2 Interpretation of Continuous Auditing Results

7.2.1 Once the tests have been run, the IT audit and assurance professional should review the results to identify where problems exist. Control weaknesses are evidenced by transactions that fail the control tests. Increased levels of risk can be identified by comparative analysis (i.e., comparing one process to other processes, one entity to other entities, or running the same tests and comparing results over time). One of the practical challenges of implementing a continuous auditing or monitoring system is the efficient response to control exceptions and risks that are identified. When a continuous auditing or monitoring system is first implemented, it is not unusual for a large number of exceptions to be identified that, upon investigation, prove not to be a concern. The continuous auditing system needs to allow the test parameters to be adjusted so that, where appropriate, such exceptions do not result in alerts or notifications. Once the process of identifying such false-positives is performed, the system increasingly can be relied upon to only identify control deficiencies or risks of significant concern. In addition, the nature of the audit response to the identified transactions will vary, and not all will require an audit or immediate action. The results should be prioritised and acted upon accordingly. Details to be maintained should include:

- The results obtained
- Decisions regarding what action will be taken
- Who was notified and when
- The expected response date

7.3 Management Action

7.3.1 If a continuous auditing finding is referred to management, the IT audit and assurance professional should also request a management response outlining the action plan and date. Once the appropriate action has been taken, the IT audit and assurance professional should run the continuous auditing test again to see if the remediation has addressed the control weakness or reduced the level of risk. Subsequent tests should not identify the same problem.

7.4 Fine-tuning Continuous Assurance Routines

7.4.1 The use of a properly designed continuous auditing application will assist the audit activity in its role of providing assurance that management is maintaining an effective control framework and actively managing risk. However, continuous auditing must remain flexible and responsive to changes in the exposures and the control environment. It is not something that can be implemented and left alone for months. The IT audit and assurance professional should review the efficiency and effectiveness of the continuous auditing program periodically. Additional control points or risk exposures may need to be added, and others may be dropped. Thresholds and control tests and parameters for various analytics may need to be tightened or relaxed. During this review, the IT audit and assurance professional should also ensure that the results from continuous auditing are included in other management activities, such as enterprise resource management (ERM), balanced scorecard, and performance measurement and monitoring activities.

7.5 Documentation of Continuous Assurance Results

7.5.1 The continuous auditing process should be sufficiently documented to provide adequate audit evidence.

7.5.2 Specifically, the audit working papers should contain sufficient documentation to describe the continuous auditing routines, including the details set out in the following sections.

7.6 Planning Documentation

7.6.1 Documentation should include:

- Continuous auditing objectives
- Continuous auditing routines to be used
- An assessment of the continuous monitoring process owned by management
- Controls to be exercised
- Staffing and timing
- Who is getting the report

7.7 Execution Documentation

7.7.1 Documentation should include:

- Preparation and testing procedures and controls for the continuous auditing routines
- Details of the tests performed by the continuous auditing routines
- Details of inputs (e.g., data used, file layouts), processing (e.g., high-level flowcharts, logic) and outputs (e.g., log files, reports)
- Lists of relevant parameters or source code

7.8 Audit Evidence Documentation

7.8.1 The usual standard of documentation of audit evidence should apply to a continuous auditing assignment. Documentation should include:

- Output produced
- Description of the audit or an analysis of the audit work performed on the output
- Audit findings
- Audit conclusions
- Audit recommendations

7.8.2 Data and files used should be stored in a secure location.

8. REPORTING

8.1 Time Between Fieldwork Completion and Date of Report

8.1.1 In the traditional audit model (used by both internal and external auditors), a period of time passes between the completion of fieldwork and issuance of the related audit report. In many instances, the impact of this delay in issuance makes the information contained in the report less useful or beneficial to the user. This is a result of the aging of the information contained in the report that can be affected by such issues as auditee corrections to identified deficiencies or further deterioration to the control environment (or related auditee data) resulting from identified control weaknesses or deficiencies.

8.2 Continuous Assurance Reporting

8.2.1 Continuous auditing, therefore, is designed to enable IT audit and assurance professionals to report on subject matter within a much shorter time frame than under the current model. Theoretically, in some environments, it should be possible to shorten the reporting time frame to provide almost instantaneous or truly continuous assurance. The reporting process needs to be defined with stakeholders to ensure a more timely response and reporting of issues arising from continuous assurance exercises. Critical issues should be reported as soon as possible.

8.2.2 By definition, continuous auditing requires a higher degree of reliance on an auditee's information systems than traditional auditing requires. This is a result of the need to rely upon system-generated information vs. externally produced information as the basis for audit testing. Hence, IT audit and assurance professionals need to make judgements on both the quality of the auditee's systems as well as the information produced by the system itself. Systems that are of lower quality, or produce less-reliable information, (and require a higher degree of manual intervention) are less conducive to continuous auditing than those that are of high quality and produce reliable information.

8.2.3 Environments that are of a higher quality and produce reliable information are better suited to reporting periods of a short to continuous duration. Environments that are of a lower quality or produce less-reliable information should use longer reporting periods to compensate for the period of time that must pass for users to review and approve or correct information processed by the system.

8.3 Description of Continuous Assurance

8.3.1 The objectives, scope and methodology section of the report should contain a clear description of the continuous assurance process used. This description should be sufficiently detailed and should provide a good overview for the reader.

8.3.2 The description of the continuous auditing routine's objectives should also be included in the body of the report, where the specific finding related to the use of the routine is discussed.

8.3.3 If the description of the routine used is applicable to several findings, or is too detailed, it should be discussed briefly in the objectives, scope and methodology section of the report and the reader referred to an appendix with a more detailed description.

9. EFFECTIVE DATE

9.1 This guideline is effective for all IT audits beginning 1 May 2010.

10. REFERENCES

10.1 The Institute of Internal Auditors, 'Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment, Global Technology Audit Guide', USA, 2005

11. ACKNOWLEDGEMENTS

11.1 Kevin Mar Fan, CISA, CA, Brisbane City Council, Australia, assisted with the development of this guideline.

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: *http://www.isaca.org*

