IS Audit and Assurance Guideline
2205 Evidence

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 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).

<table>
<thead>
<tr>
<th>ISACA 2013-2014 Professional Standards and Career Management Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steven E. Sizemore, CISA, CIA, CGAP, Chairperson</td>
</tr>
<tr>
<td>Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP</td>
</tr>
<tr>
<td>Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA</td>
</tr>
<tr>
<td>Alisdair McKenzie, CISA, CISSP, ITCP</td>
</tr>
<tr>
<td>Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP</td>
</tr>
<tr>
<td>Kazumi Sakagawa, CISA, CRISC, PMP</td>
</tr>
<tr>
<td>Ian Sanderson, CISA, CRISC, FCA</td>
</tr>
<tr>
<td>Timothy Smith, CISA, CISSP, CPA</td>
</tr>
<tr>
<td>Todd Weinman, CISA, CISSP, CPA</td>
</tr>
<tr>
<td>Texas Health and Human Services Commission, USA</td>
</tr>
<tr>
<td>HP Enterprise Security Services, UK</td>
</tr>
<tr>
<td>Myers and Staufffer LC, USA</td>
</tr>
<tr>
<td>JIEC Co. Ltd., Japan</td>
</tr>
<tr>
<td>NATO, Belgium</td>
</tr>
<tr>
<td>LPL Financial, USA</td>
</tr>
<tr>
<td>The Weinman Group, USA</td>
</tr>
</tbody>
</table>
IS Audit and Assurance Guideline 2205 Evidence

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 obtaining sufficient and appropriate evidence, evaluating the received evidence and preparing appropriate audit documentation.
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 1203 Performance and Supervision
1.2.2 Standard 1205 Evidence
1.2.3 Standard 1206 Using the Work of Other Experts

1.3 Term 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 Types of evidence
2.2 Obtaining evidence
2.3 Evaluating evidence
2.4 Preparing audit documentation
2.1 Types of Evidence

2.1.1 When planning and performing an engagement, professionals should consider the types of evidence to be gathered, its use to meet engagement objectives, and its varying levels of reliability. The various types of evidence that professionals should consider using include:

- Observed processes and existence of physical items
- Documentary evidence
- Representations
- Analysis

2.1.2 Observed processes and existence of physical items can include observations of activities, property and IS functions, such as:

- A network security monitoring system in operation
- An inventory of media in an offsite storage location

2.1.3 Documentary evidence, recorded on paper or other media, can include:

- Written policies and procedures
- Results of data extractions
- Records of transactions
- Programme listings
- Other documents and records produced in the ordinary course of business

2.1.4 Written and oral representations of those being audited can include:

- Written statement by management, e.g., representations about the existence and effectiveness of internal controls or plans for a new financial system implementation
- Oral representation of such things as how a process works or plans for management follow up on actions related to the security awareness programme

2.1.5 The results of analysing information through comparisons, simulations, calculations and reasoning can also be used as evidence. Examples include:

- Benchmarking IS performance against other enterprises or past periods
- Comparison of error rates between applications, transactions and users
- Reperformance of processes or controls

2.2 Obtaining Evidence

2.2.1 Professional should obtain sufficient and appropriate evidence to allow them to draw reasonable audit conclusions. This evidence includes:

- The procedures performed
- The results of the procedures performed
- Source documents (in either electronic or paper format), records and corroborating information used to support the audit engagement
- Documentation that the work was performed and complies with applicable laws, regulations and policies

2.2.2 Where evidence obtained in the form of oral representations is critical to the audit opinion or conclusion, professionals should consider obtaining confirmation of the representations, either in writing or electronically (such as through email). Professionals should also consider alternative evidence to corroborate these representations to ensure their reliability.
2.2 Obtaining Evidence cont.  

2.2.3 When gathering evidence, the professional should consider the following:

- The time, level of effort and cost of obtaining the evidence compared to the sufficiency of the evidence in reducing audit risk
- Significance of the matter being evaluated and of the audit procedure requiring the evidence in achieving the audit objectives and reducing audit risk
- Electronic evidence may not be retrievable in whole or in part after the passage of time

2.2.4 Procedures used to gather evidence vary depending on the characteristics of the information system being audited, timing of the audit, audit scope and objectives, and professional judgement. Evidence can be gathered through the use of manual audit procedures, computer-assisted audit techniques (CAATs) or a combination of both. Professionals should select the most appropriate procedure in relation to the IS audit objective. The following procedures should be considered:

- **Inquiry and confirmation**—The process of seeking information from experienced people who are familiar with the subject matter. The experienced people need not be members of the enterprise being audited. This procedure can range from formal written inquiries to informal oral inquiries.

- **Observation**—Observing a procedure or process being performed by those individuals who are typically responsible for its performance, or observing physical items such as facilities, computer hardware, or information system settings or configurations. This type of evidence is limited to the point in time at which the observation took place. Professionals should take into account that observing the performance of a process or procedure may affect how the procedure or process is being performed.

- **Inspection**—Examination of internal or external documents and records. The items to be inspected can be supplied in paper or electronic form. Inspection can also include physical asset examination.

- **Analytical procedures**—Evaluating (financial or non-financial) data by examining possible relationships within the data or between the data and other relevant information. This also includes the examination of fluctuations, trends and inconsistent relationships.

- **Recalculation/computation**—The process of checking the arithmetical and mathematical accuracy of documents or records. This can be performed manually or through the use of CAATs.

- **Reperformance**—Independent performance of procedures and/or controls that were originally executed by the information system or by the enterprise itself.

- **Other generally accepted methods**—Other generally accepted procedures that can be followed by professionals in gathering sufficient and appropriate evidence. For example, professionals can perform social engineering, act as a mystery guest or conduct ethical intrusion testing.

2.2.5 When gathering evidence, professionals should consider the independence and qualifications of the provider of the audit evidence. For example,
2.2 Obtaining Evidence cont

corroborative audit evidence from an independent third party can be more reliable than audit evidence obtained from the enterprise being audited. Physical audit evidence is generally more reliable than the representations of an individual.

2.2.6 If there is a possibility that the gathered evidence will become part of a legal proceeding, professionals should consult with the appropriate legal counsel to determine whether there are any special requirements that will impact the way evidence needs to be gathered, presented and disclosed.

2.2.7 In situations where professionals are not able to obtain sufficient audit evidence, such as when individuals or management refuse to provide sufficient and appropriate evidence necessary to achieve the IS audit objectives, professionals should disclose this situation to audit management, and if necessary to those charged with governance. Professionals should also disclose this fact in accordance with the audit organisation’s established procedures. Restriction or limitations on the scope of the audit and achievement of the audit objectives should also be disclosed in the communication of the audit results.

2.2.8 Professionals should retain evidence after completion of the audit work to ensure that the evidence is:

- Available for a time period and in a format that complies with the audit organisation’s policies and relevant professional standards, laws and regulations
- Protected from unauthorised disclosure or modification throughout its preparation and retention
- Properly disposed of at the end of the retention period

2.3 Evaluating Evidence

2.3.1 Evidence is sufficient and appropriate when it provides a reasonable basis for supporting the findings or conclusions within the context of the audit objectives. If, in professionals’ judgement, the evidence does not meet these criteria, they should obtain additional evidence or perform additional procedures to reduce the limitations or uncertainties related to the evidence. For example, a programme listing may not be adequate evidence until other evidence has been gathered to verify that it represents the actual programme used in the production process.

2.3.2 When evaluating reliability of evidence obtained during the audit, professionals should consider the characteristics and properties of the evidence, such as its source, nature (written, oral, visual or electronic), authenticity (presence of digital or manual signatures, date/time stamps), and relationships between evidence that provide corroborating evidence from multiple sources. In general, the reliability of evidence is ranked from low to high based on the procedures used to obtain the evidence as follows:

- Inquiry and confirmation
- Observation
- Inspection
- Analytical procedures
- Recalculation or computation
- Reperformance
2.3 Evaluating Evidence cont.

For each of the previous procedures, evidence reliability is generally greater when it is:
- In written form, rather than obtained from oral representations
- Obtained directly by the professionals rather than indirectly by the entity being audited
- Obtained from independent sources
- Certified by an independent party
- Maintained by an independent party

2.3.3 Professionals should consider the period of time during which information exists or is available in determining the nature, timing and extent of substantive testing and, if applicable, compliance testing. For example, evidence processed by electronic data interchange (EDI), document image processing (DIP) and dynamic systems such as spreadsheets may not be retrievable after a specified period of time if changes to the files are not controlled or the files are not backed up. Documentation availability could also be impacted by the enterprise document retention policies.

2.3.4 If there is an independent third-party audit, professionals should consider whether testing of controls relevant to the subject of the audit was performed and whether any reliance can be placed on the results of that testing.

2.3.5 Professionals should obtain evidence that is sufficient and appropriate to enable a qualified independent party to reperform the tests and obtain the same results and conclusions.

2.4 Preparing Audit Documentation

2.4.1 During the performance of the audit, professionals should prepare documentation of the evidence obtained to be retained and available during a predefined time period and in a format that complies with enterprise policies and relevant professional standards, laws and regulations.

2.4.2 Evidence obtained during the performance of the audit should be appropriately identified, cross-referenced, and catalogued to facilitate determining the overall sufficiency and appropriateness of evidence to provide a reasonable basis for the findings and conclusions within the context of the audit objectives and to allow for easy retrieval by other IS audit team members or an independent party.

2.4.3 Professionals should ensure that documentation of evidence is protected from unauthorised access, disclosure or modification throughout its preparation and retention.

2.4.4 Professionals should dispose of evidence documentation at the end of the established retention period.

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 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.

<table>
<thead>
<tr>
<th>Standard Title</th>
<th>Relevant Standard Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1203 Performance and Supervision</td>
<td>IS audit and assurance professionals shall obtain sufficient and appropriate evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.</td>
</tr>
<tr>
<td></td>
<td>IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions.</td>
</tr>
<tr>
<td>1205 Evidence</td>
<td>IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results.</td>
</tr>
<tr>
<td></td>
<td>IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.</td>
</tr>
<tr>
<td>1206 Using the Work of Other Experts</td>
<td>IS audit and assurance professionals shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.</td>
</tr>
</tbody>
</table>

3.2 Linkage to COBIT 5 Processes

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

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

<table>
<thead>
<tr>
<th>COBIT 5 Process</th>
<th>Process Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEA02 Monitor, evaluate and assess the system of internal controls.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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
3.3 Other Guidance cont.
- Management
- Governance bodies within the enterprise, e.g., audit committee
- Professional organisations or professional media groups
- Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriate evidence</td>
<td>The measure of the quality of the evidence</td>
</tr>
<tr>
<td>Representation</td>
<td>A signed or oral statement issued by management to professionals, where management declares that a current or future fact (e.g., process, system, procedure, policy) is or will be in a certain state, to the best of management’s knowledge</td>
</tr>
<tr>
<td>Sufficient evidence</td>
<td>The measure of the quantity of evidence; supports all material questions to the audit objective and scope. See evidence.</td>
</tr>
</tbody>
</table>

5. Effective Date

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