IS Audit and Assurance Guideline
2201 Engagement Planning

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).

<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.IISP</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>Katsumi 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</td>
</tr>
</tbody>
</table>
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 This guideline provides guidance to the IS audit and assurance professionals. Adequate planning helps to ensure that appropriate attention is devoted to important areas of the audit, potential problems are identified and resolved on a timely basis, and the audit engagement is properly organised, managed and performed in an effective and efficient manner.

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 1201 Engagement Planning
1.2.2 Standard 1202 Risk Assessment in Audit Planning
1.2.3 Standard 1203 Performance and Supervision
1.2.4 Standard 1204 Materiality

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 IS audit plan
2.2 Objectives
2.3 Scope and business knowledge
2.4 Risk-based approach
2.5 Documenting the audit engagement project plan
2.6 Changes during the course of the audit
2.1 IS Audit Plan

2.1.1 For an audit function, a comprehensive risk-based IS audit plan should be developed and updated, at least annually. A multi-annual (three to five years) time horizon should be established and incorporated into the annual plan. The multi-annual and annual plans should act as a framework for IS audit and assurance activities and serve to address responsibilities set by the audit charter.

2.1.2 The IS audit plan should be prepared so that it is in compliance with any appropriate external requirements in addition to the current ISACA standards.

2.1.3 Each audit engagement should be referenced either to the IS audit plan or state the specific mandate, objectives and other relevant aspects of the work to be performed.

2.2 Objectives

2.2.1 Professionals should define the audit engagement objectives and document them in the audit engagement project plan, so that they will be performed in an effective manner. The engagement objectives should be established to address the risk associated with the activity under review.

2.2.2 Professionals should develop an audit engagement project plan that takes into consideration the objectives of the audit engagement. These objectives might influence the audit engagement, e.g., resources needed, timeline and deliverables.

2.3 Scope and Business Knowledge

2.3.1 Before beginning an audit engagement, the work of professionals should be planned in a manner appropriate for meeting the audit objectives. As part of the planning process, professionals should obtain an understanding of the enterprise and its processes. This will assist them in determining the significance of the resources being reviewed as they relate to the objectives of the enterprise. In this way, professionals can focus on the areas most sensitive to fraudulent or inaccurate practices. They should establish the scope of the audit work and also perform a preliminary assessment of the internal controls over the function being reviewed.

2.3.2 Professionals should gain an understanding of the types of personnel, events, transactions and practices that can have a significant effect on the specific enterprise, function, process or data that is the subject of the audit engagement. Knowledge of the enterprise should include the business and financial risk facing the enterprise as well as conditions in the enterprise marketplace and the extent to which the enterprise relies on outsourcing to meet its objectives. Professionals should use this information in identifying potential problems, formulating the objectives and scope of the work, performing the work, and considering actions of management for which they should be alert.

2.4 Risk-based Approach

2.4.1 Professionals should develop an audit engagement project plan to reduce audit risk to an acceptable level.
2.4 Risk-based Approach cont.

2.4.2 A risk assessment should be performed to provide reasonable assurance that all material items will be covered adequately during the audit engagement and that professionals will be able to come to a conclusion. This assessment should identify areas with relatively high probability of material problems.

2.4.3 A risk assessment and prioritisation of identified risk for the area under review and the enterprise IS environment should be carried out to the extent necessary.

2.4.4 Normally in the planning process, professionals should establish levels of planning materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently. For example, in the review of an existing system, professionals should evaluate materiality of the various components of the system in planning the audit engagement for the work to be performed. Both qualitative and quantitative aspects should be considered in determining materiality.

2.4.5 Before beginning an audit engagement and in the course of the audit, the professionals should consider compliance with applicable laws and professional auditing standards.

2.4.6 When professionals evaluate internal controls for the purpose of placing reliance on control procedures in support of information being gathered as part of a larger audit exercise (such as an audit of historical financial information), they should, as a rule, make a preliminary evaluation of the controls and develop the audit engagement project plan on the basis of this evaluation.

2.5 Documenting the Audit Engagement Project Plan

2.5.1 Professionals’ work papers should include the audit engagement project plan.

2.5.2 A clear project definition is a critical success factor to ensure project effectiveness and efficiency. An audit engagement project plan should include in the terms of reference items such as:

- Areas to be audited
- Type of work planned
- High-level objectives and scope of the work
- Fact-finding interviews to be conducted
- Relevant information to be obtained
- Procedures to verify or validate the information obtained and their use as audit evidence
- General topics, e.g.:
  - Budget
  - Resource availability and allocation
  - Schedule dates
  - Type of report
  - Intended audience
  - Deliverables
- Specific topics, e.g.:
  - Identification of tools needed for gathering evidence, performing tests and preparing/summarising information for reporting
  - Assessment criteria to be used
  - Reporting requirements and distribution
2.5 Documenting the audit Engagement Project Plan cont.

- Other general aspects of the work, when applicable

2.5.3 The project plan should include the requirements related to the timeline of the audit engagement, such as the period covered and the different completion dates, to perform the audit engagement within the agreed-on schedule. This also includes budgetary expenditure.

2.5.4 Professionals should ensure full coverage of the required competencies by the resources of the audit engagement. They should set up an audit engagement team that has the right skills, knowledge and experience to successfully complete the audit engagement. The professionals should make sure to assign the different roles and responsibilities to the IS audit team members that best match with their competencies. For more information refer to Standard 1203 Performance and Supervision.

2.5.5 The audit engagement project plan should list all deliverables that are linked to the audit engagement.

2.5.6 The audit engagement project plan and any subsequent changes to this plan should be approved by the IS audit and assurance management.

2.5.7 After approval by the IS audit and assurance management, parts of the audit engagement project plan (e.g., scope, timeline, document requirements, interview schedule) should be timely communicated towards the auditees for them to provide appropriate and complete access and availability to the needed documents and resources.

2.6 Changes During the Course of the Audit

2.6.1 The audit engagement project plan should be updated and changed as necessary during the course of the audit engagement.

2.6.2 Planning an audit engagement is a continual and iterative process. As a result of unexpected events, changes in conditions or the audit evidence obtained, professionals may need to modify the planned nature, timing and extent of further audit procedures.

2.6.3 The audit plan should consider the possibility of unexpected events that imply risk for the enterprise. Accordingly, the audit engagement project plan should be able to prioritise such events within the audit and assurance processes based on risk.

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 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

**1201 Engagement Planning**

IS audit and assurance professionals shall plan each IS audit and assurance engagement to address:

- Objective(s), scope, timeline and deliverables
- Compliance with applicable laws and professional auditing standards
- Use of a risk-based approach, where appropriate
- Engagement-specific issues
- Documentation and reporting requirements

IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the:

- Engagement nature, objectives, timeline and resource requirements
- Timing and extent of audit procedures to complete the engagement

### Relevant Standard Statements

<table>
<thead>
<tr>
<th>Standard Title</th>
<th>Relevant Standard Statements</th>
</tr>
</thead>
</table>
| 1201 Engagement Planning | IS audit and assurance professionals shall plan each IS audit and assurance engagement to address:  
  - Objective(s), scope, timeline and deliverables  
  - Compliance with applicable laws and professional auditing standards  
  - Use of a risk-based approach, where appropriate  
  - Engagement-specific issues  
  - Documentation and reporting requirements  

IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the:  
- Engagement nature, objectives, timeline and resource requirements  
- Timing and extent of audit procedures to complete the engagement |

| 1202 Risk Assessment in Audit Planning | The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources. |

IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements. |

| 1203 Performance and Supervision | IS audit and assurance professionals shall conduct the work in accordance with the approved IS audit plan to cover identified risk and within the agreed-on schedule. |

| 1204 Materiality | IS audit and assurance professionals shall consider potential weaknesses or absences of controls while planning an engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness. |

#### 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**.

<table>
<thead>
<tr>
<th>COBIT 5 Process</th>
<th>Process Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEA01 Monitor, evaluate and assess performance and conformance.</td>
<td>Provide transparency of performance and conformance and drive achievement of goals.</td>
</tr>
<tr>
<td>MEA02 Monitor, evaluate and assess the system of internal control.</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>
<tr>
<td>MEA03 Monitor, evaluate and assess compliance with external requirements.</td>
<td>Ensure that the enterprise is compliant with all applicable external requirements.</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 organisation and/or outside the enterprise, e.g., through professional associations or professional social media groups
- Management
- Governance bodies within the organisation, e.g., audit committee
- Other guidance (e.g., books, papers, other guidelines)

4. Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Audit plan         | 1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion.  
Scope Notes: Includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work  
2. A high-level description of the audit work to be performed in a certain period of time. |
| Audit risk         | The risk of reaching an incorrect conclusion based upon audit findings. The three components of audit risk are:  
- Control risk  
- Detection risk  
- Inherent risk |
| Materiality        | An audit concept regarding the importance of an item of information with regard to its impact or effect on the subject matter being audited. An expression of the relative significance or importance of a particular matter in the context of the engagement or the enterprise as a whole. |
| Risk assessment    | A process used to identify and evaluate risk and its potential effects.  
Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan.  
Risk assessments are also used to manage the project delivery and project benefit risk. |

5. Effective Date

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