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](http://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 to design and select an audit sample and evaluate sample results. Appropriate sampling and evaluation will help in achieving the requirements of sufficient and appropriate evidence.

1.1.2 IS audit and assurance professionals should consider this guideline when determining how to implement related standards, 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 1006 Proficiency
1.2.2 Standard 1202 Risk Assessment in Planning
1.2.3 Standard 1203 Performance and Supervision
1.2.4 Standard 1205 Evidence

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 Sampling
2.2 Design of the sample
2.3 Selection of the sample
2.4 Evaluation of sample results
2.5 Documentation
2.1 Sampling

2.1.1 In forming an opinion or conclusion, professionals frequently do not examine all of the information available as it may be impractical (e.g., requiring too much time for both the auditee as well as professionals to investigate all information) and valid conclusions can be reached using audit sampling.

2.1.2 When using either statistical or non-statistical sampling methods, the professionals should design and select an audit sample, perform audit procedures and evaluate sample results to obtain sufficient and appropriate evidence to form a conclusion. When using sampling methods to draw a conclusion on the entire population, professionals should use statistical sampling.

2.2 Design of the Sample

2.2.1 When designing the size and structure of an audit sample, professionals should consider the specific IS audit objectives, the audit procedures that are most likely to achieve those objectives, the nature of the population, relevant subgroups within the population, and the sampling and selection methods. In addition, when audit sampling is appropriate, consideration should be given to the nature of the evidence sought, possible error conditions and possible root causes.

2.2.2 When designing the audit sample, while taking into account the IS audit objectives professionals should consider:

- Purpose of the sample
- Sampling unit
- Population
- Sampling risk and sample size
- Tolerable error
- Underlying expected distribution (e.g., Poisson, binomial, normal, exponential)
- Behaviour over time (e.g., seasonality, decrement in performance)
- Subpopulations or subgroups that are naturally occurring and should be considered for operational relevance
- Outliers
- Small populations of adverse or rare events
- Data from external support tools, used to confirm or complement the results of sampling

2.2.3 Professionals should consider the purpose of the sample:

- Compliance testing/test of controls—An audit procedure designed to evaluate the operating effectiveness of controls in preventing or detecting and correcting material weaknesses. Examples of compliance testing of controls, where sampling could be considered, include user access rights, program change control procedures, procedure documentation, program documentation, follow-up on exceptions, review of logs and software licences audits.
- Substantive testing/test of details—An audit procedure designed to detect material weaknesses at the assertion level. Examples of
2.2 Design of the Sample cont. substantive tests, where sampling could be considered, include reperformance of a complex calculation (e.g., interest) on a sample of accounts, a sample of transactions to vouch to supporting documentation, etc.

2.2.4 The sampling unit depends on the purpose of the sample. For compliance testing of controls, where the sampling unit is an event or transaction (e.g., a control such as authorisation of an invoice), attribute sampling is typically applied as it is used to determine the characteristics of a population. For substantive testing, where the sampling unit is often monetary, variables sampling is frequently applied because it is used to determine the monetary or volumetric impact of characteristics of a population.

2.2.5 The population is the entire set of data from which professionals wish to sample to reach a conclusion on the population. Therefore, the population from which the sample is drawn has to be appropriate to test the design and/or operating effectiveness of the controls, and verified as complete for the specific IS audit objective and scope.

2.2.6 To assist in the efficient and effective design of the sample, sampling stratification may be appropriate. Stratification is the process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum.

2.2.7 When determining sample size, professionals should consider the sampling risk, the amount of the error that would be acceptable and the extent to which errors are expected. Sampling risk arises from the possibility that professionals’ conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risk:

- **The risk of incorrect acceptance**—A material weakness is assessed as unlikely when, in fact, the population is materially misstated.
- **The risk of incorrect rejection**—A material weakness is assessed as likely when, in fact, the population is not materially misstated.

2.2.8 Sample size is affected by the level of sampling risk that the professionals are willing to accept. Sampling risk should also be considered in relation to the audit risk model and its components, inherent risk, control risk, and detection risk, as detailed in Standard 2202 Risk Assessment in Planning.

2.2.9 Tolerable error is the maximum error in the population that professionals are willing to accept and still conclude that the test objective has been achieved. For substantive tests, tolerable error is related to professionals’ judgement about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that professionals are willing to accept.

2.2.10 If professionals expect errors to be present in the population, a larger sample than when no error is expected has to be examined to conclude that the actual error in the population is not greater than the expected tolerable error. Smaller sample sizes are justified when the population is expected to be error free. When estimating the expected error in a population, professionals should consider such matters as:

- Error levels identified in previous audits
- Changes in enterprise procedures
Evidence available from an evaluation of the system of internal control, results from analytical review procedures, and/or results of preliminary tests of the population.

2.2.11 Professionals should consider, if appropriate, the need to involve specialists in the design and analysis of complex sampling approaches, such as stratified random samples that must have statistical validity, or sampling based in established quality control methods (e.g., Six Sigma).

2.2.12 Should professionals conclude that sampling does not allow achieving the IS audit objectives and a test of the entire population is required, they should consider applying continuous assurance because it allows testing of the entire population in a timely and cost-effective way.

2.3 Selection of the Sample

2.3.1 Professionals should ensure that the population is complete and control the selection of the sample, to maintain audit independence. Professionals should select sample items in such a way that the sample is expected to be representative of the population regarding the characteristics being tested.

2.3.2 For a sample to be representative of the entire population, all sampling units in the population should have an equal or known, non-zero probability of being selected. This implies using statistical sampling methods, because they involve the use of techniques from which mathematically constructed conclusions regarding the entire population can be drawn. Professionals should thus validate completeness of the population to ensure that the sample is selected from an appropriate data set.

2.3.3 Non-statistical sampling is an approach used by professionals who want to use their own experience, knowledge and professional judgement to determine a sample. This method implies a human bias because it is not statistically based, does not ensure that every sampling unit has a known, non-zero probability of being selected, and thus results should not be extrapolated over the population because the sample is unlikely to be representative of the entire population. Non-statistical sampling may be used when results are needed quickly to confirm a proposition and should not be used to draw mathematically constructed conclusions regarding the entire population.

2.3.4 There are five commonly used sampling methods, divided into either statistical sampling methods or non-statistical sampling methods:

- Statistical sampling methods are:
  - **Simple random sampling**—Ensures that all combinations of sampling units in the population have an equal chance of selection
  - **Systematic sampling**—Involves selecting sampling units using a fixed interval between selections, the first interval having a random start. Examples include Monetary Unit Sampling or Value Weighted selection where each individual monetary value (e.g., $1000) in the population is given an equal chance of selection. Because ordinarily the individual monetary unit cannot be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weighs the selection in favour of the larger amounts. Another example includes selecting every ‘nth’
2.3 Selection of the Sample cont.

- Stratified random sampling—Ensures that all sampling units in each subgroup have a known, non-zero chance of selection.

Professionals should consider using statistical software for calculating standard deviations and other summary statistics for results of statistical sampling.

- Non-statistical sampling methods are:
  - Haphazard sampling—Professionals select the sample without following a structured technique, while avoiding any conscious bias or predictability. However, analysis of a haphazard sample should not be relied upon to form a conclusion on the population.
  - Judgemental sampling—Professionals place a bias on the sample (e.g., all sampling units over a certain value, all for a specific type of exception, all negatives). It should be noted that a judgemental sample is not statistically based and results should not be extrapolated over the population because the sample is unlikely to be representative of the population as a whole.

2.3.5 There are two commonly used selection methods:

- Selection on records and population subgroups; common methods are:
  - Simple random sampling
  - Stratified random sampling
  - Haphazard sampling
  - Judgemental sample

- Selection on quantitative fields (e.g., monetary units); common methods are:
  - Simple random sampling
  - Systematic sampling

2.4 Evaluation of Sample Results

2.4.1 Having performed those audit procedures that are appropriate to the particular IS audit objective on each sample item, professionals should analyse any possible errors detected in the sample to determine whether they are actually errors and, if appropriate, the nature and cause of the errors. For those that are assessed as actual errors, the errors should be projected as appropriate to the population, but only if the sampling method used is statistically based.

2.4.2 Any possible errors detected in the sample should be reviewed to determine whether they are actually errors. Professionals should consider the qualitative aspects of the errors. These include the nature and cause of the error and the possible effect of the error on the other phases of the audit. For example, errors that are the result of the breakdown of an automated process normally have wider implications than human errors.

2.4.3 When the expected audit evidence regarding a specific sample unit cannot be obtained, professionals should consider whether they are able to obtain sufficient and appropriate audit evidence by performing alternative procedures on the item selected, or by selecting and testing a replacement sample unit.
2.4 Evaluation of Sample Results cont.

2.4.4 Professionals should consider projecting the results of the sample to the population with a method of projection consistent with the method used to select the sampling unit. The projection of the sample may involve estimating the probable error in the population, and estimating any further error that might not have been detected because of the imprecision of the technique, together with the qualitative aspects of any errors found.

2.4.5 Discussion of the results of non-statistical sampling (haphazard or judgmental) should be restricted to a description of the results of analyzing the sample, in context of the population as a whole.

2.4.6 Professionals should consider whether errors in the population might exceed the tolerable error by comparing the projected population error to the estimated or defined tolerable error, taking into account the results of other audit procedures relevant to the audit objective. Tolerable error may be estimated or defined by audit criteria, industry standards, contractual requirements, software specifications, etc. When the projected population error exceeds the tolerable error, professionals should reassess the sampling risk and, if that risk is unacceptable, consider extending the audit procedure, recalculating sample size using the refined tolerable error and testing the additional sample units, or performing alternative audit procedures.

2.5 Documentation

2.5.1 The work papers should include sufficient detail to describe clearly the sampling objective and the sampling process used. The work papers should include:

- Purpose of the sample, including sample unit
- Source of the population, definition of the population, and its relation to the audit scope
- Sampling parameters, e.g., sample size (including any consideration with regards to sampling risk), random start or seed number or method by which random start was obtained, sampling interval
- Sampling method
- Items selected and, if non-statistical sampling is used, justification for the selected items
- Details of audit tests performed, including evaluation of errors and, if applicable, alternative audit procedures
- Conclusions reached

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 Seek 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.

<table>
<thead>
<tr>
<th>Standard Title</th>
<th>Relevant Standard Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1006 Proficiency</td>
<td>IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate skills and proficiency in conducting IS audit and assurance engagements and be professionally competent to perform the work required.</td>
</tr>
<tr>
<td>1202 Risk Assessment in Planning</td>
<td>IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.</td>
</tr>
<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 shall be supported by appropriate analysis and interpretation of this evidence. IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions. IS audit and assurance professionals shall identify and conclude on findings.</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. IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.</td>
</tr>
</tbody>
</table>

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>APO12 Manage risk.</td>
<td>Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.</td>
</tr>
</tbody>
</table>
| 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
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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute sampling</td>
<td>Method to select a portion of a population based on the presence or absence of a certain characteristic</td>
</tr>
<tr>
<td>Audit sampling</td>
<td>The application of audit procedures to less than 100 percent of the items within a population to obtain audit evidence about a particular characteristic of the population</td>
</tr>
<tr>
<td>Non-statistical sampling</td>
<td>Method of selecting a portion of a population, by means of own judgement and experience, for the purpose of quickly confirming a proposition. This method does not allow drawing mathematical conclusions on the entire population.</td>
</tr>
<tr>
<td>Population</td>
<td>The entire set of data from which a sample is selected and about which an IS auditor wishes to draw conclusions.</td>
</tr>
<tr>
<td>Sampling risk</td>
<td>The probability that an IS auditor has reached an incorrect conclusion because an audit sample, rather than the entire population, was tested. Scope Notes: While sampling risk can be reduced to an acceptably low level by using an appropriate sample size and selection method, it can never be eliminated.</td>
</tr>
<tr>
<td>Sampling stratification</td>
<td>The process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum</td>
</tr>
<tr>
<td>Statistical sampling</td>
<td>A method of selecting a portion of a population, by means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population.</td>
</tr>
<tr>
<td>Tolerable error</td>
<td>The maximum error in the population that professionals are willing to accept and still conclude that the test objective has been achieved. For substantive tests, tolerable error is related to professionals’ judgement about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the professionals are willing to accept.</td>
</tr>
</tbody>
</table>
IS Audit and Assurance Guideline 2208 Sampling

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable sampling</td>
<td>A sampling technique used to estimate the average or total value of a population based on a sample; a statistical model used to project a quantitative characteristic, such as a monetary amount</td>
</tr>
</tbody>
</table>

5. Effective Date and Review Date

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