IS Audit and Assurance Guideline 2202 Risk Assessment in 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).

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 level of audit work required to meet the audit objective is a subjective decision made by IS audit and assurance professionals. The purpose of this guideline is to reduce the risk of reaching an incorrect conclusion based on the audit findings and to reduce the existence of errors in the area being audited.

1.1.2 The guideline provides guidance in applying a risk assessment approach to develop an:
- IS audit plan that covers all annual audit engagements
- Audit engagement project plan that focuses on one specific audit engagement

1.1.3 The guideline provides the details of the different types of risk the IS audit and assurance professionals encounter.

1.1.4 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 Planning
1.2.3 Standard 1203 Performance and Supervision
1.2.4 Standard 1204 Materiality
1.2.5 Standard 1207 Irregularity and Illegal Acts

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

IS Audit and Assurance Guideline 2202 Risk Assessment in Planning

2.0 Introduction

The guideline content section is structured to provide information on the following key audit and assurance engagement topics:

2.1 Risk assessment of the IS audit plan
2.2 Risk assessment methodology
2.3 Risk assessment of individual audit engagements
2.4 Audit risk
2.5 Inherent risk
2.6 Control risk
2.7 Detection risk

2.1 Risk Assessment of the IS Audit Plan

2.1.1 When developing the overall IS audit plan, a suitable risk assessment approach should be followed. A risk assessment should be conducted and documented at least annually to facilitate the development process of the IS audit plan. It should take into account the organisational strategic plans and objectives and the enterprise risk management framework and initiatives.

2.1.2 To correctly and completely assess the risk that is related to the complete scope of the IS audit area, professionals should consider the following elements when developing the IS audit plan:

- Full coverage of all areas within the scope of the IS audit universe, which represents the range of all possible audit activities
- Reliability and suitability of the risk assessment provided by management
- The processes followed by management to supervise, examine and report possible risk or issues
- Cover risk in related activities relevant to the activities under review

2.1.3 The applied risk assessment approach should help with the prioritisation and scheduling process of the IS audit and assurance work. It should support the selection of areas and items of audit interest and the decision process to design and conduct particular IS audit engagements.

2.1.4 Professionals should ensure that the applied risk assessment approach is approved by those charged with governance and distributed to the various engagement stakeholders

2.1.5 Professionals should use risk assessments to quantify and justify the amount of IS audit resources needed to complete the IS audit plan and the requirements for specific engagements

2.1.6 Based on the risk assessment(s), professionals should develop an IS audit plan that acts as a framework for the IS audit and assurance activities. It should:

- Consider non-IS audit and assurance requirements and activities
- Be updated at least annually
- Be approved by those charged with governance
- Address responsibilities set by the audit charter

For more information refer to Standard 1201 Engagement Planning.

2.2 Risk Assessment Methodology

2.2.1 Professionals should consider the appropriate risk assessment methodology to ensure complete and accurate coverage of the audit engagements in the IS audit plan.

2.2.2 Professionals should at least include an analysis, within the methodology, of the risk to the enterprise related to system availability, data integrity and business information confidentiality.

2.2.3 Many risk assessment methodologies are available to support the risk assessment process. These range from simple classifications of high, medium and low, based on professionals' judgement, to more quantitative and scientific calculations providing a numeric risk rating, and others which are a combination of the two. Professionals should consider the level of complexity and detail appropriate for the enterprise or subject(s) being audited. Specific guidance on performing risk assessments can be found in the ISACA publication *COBIT 5 for Risk*.

2.2.4 All risk assessment methodologies rely on subjective judgements at some point in the process (e.g., for assigning weights to the various parameters). Professionals should identify the subjective decisions required to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.

2.2.5 In deciding which is the most appropriate risk assessment methodology, professionals should consider such things as the:

- Type of information required to be collected (some systems use financial effects as the only measure—this is not always appropriate for IS audit engagements)
- Cost of software or other licences required to use the methodology
- Extent to which the information required is already available
- Amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
- Opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits
- Willingness of those charged with governance of the IS audit area to accept the methodology as the means of determining the type and level of audit work carried out

2.2.6 No single risk assessment methodology can be expected to be appropriate in all situations. Conditions affecting audits may change over time. Periodically, professionals should re-evaluate the appropriateness of the chosen risk assessment methodologies.

2.2.7 The professionals should use the selected risk assessment techniques in developing the overall IS audit plan and in planning specific audit engagements. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as the:

- Areas or business functions to be audited
- Amount of time and resources to be allocated to an audit
- Nature, extent and timing of audit procedures

2.2.8 The risk assessment methodologies adopted should produce consistent, valid, comparable and repeatable results. Risk assessments that come out

2.2 Risk Assessment Methodology cont.

of the methodology should be consistent (over a period), valid, comparable (with earlier/later assessments using the same assessment methodology) and repeatable (given a similar set of facts, using the same assessment methodology will produce a similar outcome).

2.3 Risk Assessment of Individual Audit Engagements

2.3.1 When planning an individual engagement, professionals should identify and assess risk relevant to the area under review. The results of this risk assessment should be reflected in the audit engagement objectives. During the risk assessment, professionals should consider:

- Results of prior audit engagements, reviews and findings, including any remedial activities
- The enterprise overarching risk assessment process
- The likelihood of occurrence of a particular risk
- The impact of a particular risk (in monetary or other value measures) if it occurs

2.3.2 Professionals should ensure full understanding of the activities in scope before assessing risk. They should request comments and suggestions from stakeholders and other appropriate parties. This is needed to correctly determine and examine the impact of possible risk in the audit engagements.

2.3.3 The goal of the risk assessment is the reduction of audit risk to an acceptably low level, and identifying those parts of an activity that should receive more audit focus. This needs to be performed by an appropriate assessment of the IS subject matter and related controls, while planning and performing the IS audit.

2.3.4 When planning a specific IS audit and assurance procedure, professionals should recognise the fact that the lower the materiality threshold is, the more precise the audit expectations will be and the greater the audit risk.

2.3.5 When planning a specific IS audit and assurance procedure, professionals should consider possible illegal acts that can require a modification of the nature, timing or extent of the existing procedures. For more information refer to Standard 1207 Irregularity and Illegal Acts and Guideline 2207.

2.3.6 To gain additional assurance in instances where there is high audit risk or a lower materiality threshold, professionals should compensate by either extending the scope or nature of the IS audit tests or increasing or extending the substantive testing.

2.4 Audit Risk

2.4.1 Audit risk refers to the risk of reaching an incorrect conclusion based upon audit findings. The three components of audit risk are:

- Control risk
- Detection risk
- Inherent risk

2.4.2 Professionals should consider each of the risk components to determine the overall level of risk. This includes subject matter risk, which includes inherent risk and control risk; together with detection risk it is then referred to as audit risk. Further elaboration on the different components of audit risk can be found in sections 2.5 to 2.7.

2.5 Inherent Risk

2.5.1 Inherent risk is the susceptibility of an audit area to err in a way that could be material, individually or in combination with other errors, assuming that there were no related internal controls. For example, the inherent risk associated with operating systems without appropriate controls is ordinarily high, since changes to, or even disclosure of, data or programs through operating system security weaknesses could result in false management information or competitive disadvantage. By contrast, the inherent risk associated with security for a stand-alone PC without controls, when a proper analysis demonstrates it is not used for business-critical purposes, ordinarily is low.

2.5.2 Inherent risk for most IS audit areas is high since the potential effects of errors ordinarily spans several business systems and many users.

2.6 Control Risk

2.6.1 Control risk is the risk that an error that could occur in an audit area and could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because of the volume of logged information. The control risk associated with computerised data validation procedures ordinarily is low because the processes are applied consistently.

2.6.2 Professionals should assess the control risk as high unless relevant internal controls are:

- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

2.6.3 The professionals should consider both pervasive and detailed IS controls:

- Pervasive IS controls are considered a subset of general controls; they are those general controls that focus on the management and monitoring of the IS environment. They therefore affect all IS-related activities. The effect of pervasive IS controls on professionals' work is not limited to the reliability of application controls in the business process systems. They also affect the reliability of the detailed IS controls over, e.g., application program development, system implementation, security administration and backup procedures. Weak pervasive IS controls, and thus weak management and monitoring of the IS environment, should alert professionals to the possibility of a high risk that the controls designed to operate at the detailed level may be ineffective.
- Detailed IS controls are made up of application controls plus those general controls not included in pervasive IS controls. Following the COBIT framework, they are the controls over the acquisition, implementation, delivery and support of IS systems and services.

2.6.4 A risk that professionals should consider is the limitations and shortcomings in the detailed IS controls that are induced by inadequacies of the pervasive IS controls.

2.7 Detection Risk

2.7.1 Detection risk is the risk that professionals' substantive procedures will not detect an error that could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system ordinarily is high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with identifying a lack of disaster recovery plans ordinarily is low, since existence is verified easily.

2.7.2 In determining the level of substantive testing required, the professionals should consider the:

- Assessment of inherent risk
- Conclusion reached on control risk following compliance testing

2.7.3 The higher the assessment of inherent and control risk the more audit evidence the professionals should normally obtain from the performance of substantive audit procedures.

---

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	Relevant Standard Statements
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
1202 Risk Assessment in 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.

Standard Title	Relevant Standard Statements
	IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.
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. IS audit and assurance professionals shall consider materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures. IS audit and assurance professionals shall consider the cumulative effect of minor control deficiencies or weaknesses and whether the absence of controls translates into a significant deficiency or a material weakness. IS audit and assurance professionals shall disclose the following in the report: • Absence of controls or ineffective controls • Significance of the control deficiencies • Likelihood of these weaknesses resulting in a significant deficiency or material weakness
1207 Irregularity and Illegal Acts	IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement.

3.2 Linkage to COBIT 5 Processes

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

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

COBIT 5 Process	Process Purpose
EDM01 Ensure governance framework setting and maintenance.	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.

COBIT 5 Process	Process Purpose
EDM03 Ensure risk optimisation.	Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
APO12 Manage risk.	Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

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

- Colleagues from within the 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

Term	Definition
Audit charter	A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal IS audit and assurance activity The charter should: • Establish the internal IS audit and assurance function's position within the enterprise • Authorise access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagements • Define the scope of the IS audit and assurance function's activities
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
Control risk	The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal control. See inherent risk.

Term	Definition
Detailed IS controls	Controls over the acquisition, implementation, delivery and support of IS systems and services made up of application controls plus those general controls not included in pervasive controls
Detection risk	The risk that the IS audit or assurance professional's substantive procedures will not detect an error that could be material, individually or in combination with other errors. See audit risk.
Inherent risk	The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls). See control 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.
Pervasive IS control	General control designed to manage and monitor the IS environment and which, therefore, affects all IS-related activities
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.
Substantive testing	Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period

5. Effective Date

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

