ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

PREFACE TO THE INFORMATION SYSTEMS AUDIT STANDARDS

Contents

Paragraph(s)

1.0 Introduction and Objectives

1.1 This Preface to the Information Systems Audit Standards (referred to as "ISAS" or the "Standards") facilitates the understanding of the scope and authority of these pronouncements issued by the Digital Accounting and Assurance Board (DAAB or the "Board"), under the authority of the Council of the Institute of Chartered Accountants of India (ICAI).

1.2 The ISAS, at a broad level, seek to provide:

(a) the Professional, with the minimum standards for undertaking Information Systems Audit (ISA) engagements;

(b) the users of ISA services, with an indication of the quality of service that can be expected from such engagements;

(c) the regulators and agencies, with an appreciation of what can be expected from ISA services; and

(d) in general, guidance on matters of implementation and related practical issues.

1.3 The Standards are principle-based, thereby providing adequate scope for professional judgment when applying such principles to unique situations and under specific circumstances. The special nature and aspects associated with ISA engagements necessitates that, the application of specialised skills and the use of technical tools and techniques, may vary depending on the nature of engagement.

2.0 Digital Accounting and Assurance Board

2.1 The Council of the Institute of Chartered Accountants of India (ICAI or the "Institute"), constituted the Digital Accounting and Assurance Board (DAAB or the "Board") as a non-standing Board of the ICAI, for fostering a cohesive global strategy on aspects related to digital accounting and assurance.

2.2 The Board reviews the existing and emerging auditing and related practices and identifies areas in which standards need to be developed, and issued under the authority of the Council of the Institute.

2.3 The Board undertakes a continuous, collaborative approach in the formulation and development of the Standards. However, given the pace of digital transformation of businesses, increasing technological complexity and rapidly evolving information systems and cybersecurity landscape, the body of knowledge, practices, tools and techniques keep evolving globally, necessitating an on-going ISAS development process.

3.0 Framework Governing Information Systems Audit

3.1 Each of the Standards operate within a pre-defined framework which governs the domains of ISA. The framework seeks to ensure a consistent application of basic principles, best practices and standards to achieve a high level of quality, consistent with wide range of objectives driven by the different types of ISA engagements.

3.2 The ISAS framework is an overarching document to be read along with this Preface. It consists of the Definitions and the following four key components:

(a) Basic Principles of ISA;

(b) Key Concepts;

(c) Information Systems Audit Standards (ISAS), and

(d) Guidance.

3.3 These four components are built on the of Code of Ethics of the Institute. The full Framework is explained in a separate document tilted **Framework for Information Systems Audits.**

4.0 Information Systems Audit Standards (ISAS)

4.1 The ISAS are a minimum set of requirements that apply to all members of the ICAI when conducting ISA assignments of any entity.

5.0 Mandatory Nature of Framework and Standards

5.1 The Council of the ICAI, at an appropriate time, decides to make the ISAS mandatory, and if deemed suitable, in a phased manner, from the effective date mentioned in each Standard.

5.2 The mandatory nature of the ISAS implies that while carrying out any ISA engagements, it shall be the duty of the Professional to ensure that they comply with the Standards, as read with this Preface, the Framework Governing ISAS, and the Basic Principles of ISA.

5.3 If, for any reason, and after reasonable efforts, the Professional is unable to comply with any of the requirements of the Standard, or if there is a conflict between the Standards and other mandates, such as a statutory or regulatory requirement, the ISA report (or such similar communication) shall draw attention to the material departures therefrom along with appropriate explanation.

6.0 Standard Setting Process

6.1 The DAAB develops and when appropriate, revises the Standards. Exposure Drafts (EDs) are prepared and issued to various interest groups and public at large for their inputs, feedback and comments. DAAB reviews the comments and thereafter places the appropriately revised Standards before the Council of the ICAI for its deliberation and approval. The Standards, once approved by the Council, are issued thereafter for implementation.

6.2 The detailed 6-step process is explained in Annexure 1.

7.0 Contents of the Standards

7.1 The ISAS is principle based and clearly outline the objectives of the Standard, along with essential requirements for its compliance. Professionals shall apply their best judgement in the implementation of ISAS. Implementation and Technical Guides issued by the Board provide guidance and clarification in this regard, and are recommendatory in nature.

7.2 Each Standard maintains a fixed six section format as follows:

7.2.1 **Introduction and Scope:** Brief background, definitions and scope of the Standard and its applicability.

7.2.2 **Objective:** Purpose of issuing the Standard, the desired outcome and why it is required and essential.

7.2.3 **Requirements:** The key mandates and what is critical to achieve the objective of the Standard.

7.2.4 **Explanatory Comments:** Explanation of certain parts of the Requirements which need clarity and elaboration, including any key words or terms.

7.2.5 **Documentation of Work Procedures:** Indicative list of the nature of evidence and documentation which may be expected in order to demonstrate conformance to the Standards.

7.2.6 **Effective Date:** Date from which the Standard is to be applied and made mandatory.

7.3 The ISAS, as and when issued, are classified, and numbered in a series format, as follows:

7.3.1 100 Series: Standards on Key Concepts.

7.3.2 200 Series: Standards on Engagement Planning.

7.3.3 300 Series: Standards on Executing Assignments.

7.3.4 400 Series: Standards on Specific Areas.

7.3.5 500 Series: Standards on Reporting.

7.3.6 600 Series: Standards on Quality Control.

8.0 Guidance

8.1 Guidance Notes are primarily designed to provide non-mandatory guidance on matters of implementation or clarification on their applicability in certain circumstances. They also explain how the Standard may be put into practice.

8.2 The ICAI may issue the following guides (as appropriate):

8.2.1 Implementation Guide: Best practices, methodologies, or approach on how best to apply the prescribed requirements to achieve the objectives and requirements of the ISAS.

8.2.2 Technical Guide: Clarifications as to what extent the ISAS applies in a certain situation, or in a specific industry or under unusual circumstances, considering the technical or operational uniqueness of the same and how best to achieve the objectives of the ISAS.

8.3 The Implementation and Technical Guides are recommendatory in nature and do not represent the official position of the ICAI. The Professional should ordinarily follow these recommendations except where, under specific circumstances, it may not be necessary or appropriate to do so.

Annexure 1

DETAILS OF THE STANDARD SETTING PROCESS

1. Selection of Topics and Timelines

The Digital Accounting and Standards Board (DAAB), on a continuous basis, and in consultation with its key Stakeholders, keeps identifying the broad areas in which the ISAS need to be formulated (including the review and revision of prevailing ISAS) and prepares a priority list with time lines for the issuance of the ISAS.

2. Formation of Study Group to Draft Standards

In the preparation and drafting of the ISAS, the DAAB constitutes a Study Group (SG) of professionals. In the formation of the SG, provision is made for the participation of a cross section of members of the Institute. In certain situations, the DAAB may also consider having expert professionals in the SG, who need not necessarily be members of the ICAI. The SG meetings are convened by DAAB and generally chaired by a member of the DAAB. The SG is responsible for preparing and finalizing the Exposure Draft (ED) of the Standard for deliberation by the DAAB.

3. Review of Exposure Draft of ISAS by the DAAB

The Exposure Draft (ED) of the Standard is put up to the DAAB for their review, deliberation, and approval. While formulating the ISAS, the DAAB takes into consideration the applicable laws, customs and the business environment in India. The DAAB also, where appropriate, takes into consideration international practices in ISA, to the extent they are relevant and applicable to the requirements of the ISAS. Post deliberations of the DAAB, changes are made to the draft, and the final ED is made ready for exposure to a wide set of stakeholders for their comments.

4. Exposure Draft Open for Comments for 30 days

The ED of the proposed Standard is issued for comments by the members of the Institute. The ED is also open for comments by non-members, including the regulators and other such bodies as well as the general public. The ED may also be published in the monthly Journal of the Institute and hosted on the website of the Institute wherefrom it is downloadable free of charge for comments by the members, other professionals and the public. The ED is also circulated to all the members of the Council of the ICAI, Regional Councils, and Branches of the Institute for their comments. The ED is also circulated to other external Stakeholders as listed in Annexure 2 for their comments.

The ED is normally open for comments for a period of at least 30 (thirty) days from the date exposed, but may be extended by DAAB if necessary.

5. Finalisation and Submission to ICAI Council

After taking into consideration the comments received on the ED, the DAAB will update the draft of the proposed Standard, take inputs of the SG, and finalise the Standard for consideration by the Council of the Institute.

6. ICAI Council Deliberates and Approves ISAS

The Council of the Institute will consider the final draft of the proposed ISAS and, if necessary, modify the same. The ISAS will then be issued under the authority of the Council of the Institute, who may also mandate the date from when it would be effective for implementation.

Annexure 2

LIST OF EXTERNAL STAKEHOLDERS FOR INPUTS ON EXPOSURE DRAFTS

1. Cybersecurity and IT Examination (CSITE), Reserve Bank of India
2. Securities and Exchange Board of India
3. National Critical Information Infrastructure Protection Centre
4. Department of Financial Services, Ministry of Finance
5. Insurance Regulatory Authority of India
6. Office of the Comptroller and Auditor General of India
7. Ministry of Corporate Affairs
8. Computer Emergency Response Team-India (CERT-IN), MeiTy
9. Indian Cybercrime Coordination Centre (I4C), Ministry of Home Affairs
10. National Security Council, Office of the National Security Agency
11. Financial Stability and Cybersecurity Division, Department of Economic Affairs
12. Cyber and Information Security (C&IS) Division, Ministry of Home Affairs
13. National Cyber Co-ordination Centre (NCCC)
14. Telecom Regulatory Authority of India (TRAI)

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

FRAMEWORK GOVERNING INFORMATION SYSTEMS AUDIT

Contents

Paragraph(s)

1.0 Introduction and Scope

1.1 The Framework governing Information Systems Audit (the "Framework") establishes the underlying principles and boundaries for undertaking and carrying out Information Systems Audit (ISA) services. It provides clarity on key components governing ISA to ensure standardisation and quality in discharge of Professional's responsibilities. This Framework needs to be read in conjunction with the Preface to the Information Systems Audit Standards (ISAS or the "Standards").

1.2 The Framework provides a structured and systematic design necessary for consistency, discipline and quality in discharge of responsibilities relating to practice of performing ISA responsibilities. These are foundational to the quality of ISA achieved by appropriate application of the components of the framework.

1.3 **Scope:** The framework covers all type of ISA services provided by a Professional. However, the Standards do not apply to a situation where a Professional performs audit of IS as part of an assurance engagement such as Statutory audit or any other attest engagement where the audit objective does not specifically include audit of information systems and is governed by specific laws and regulations thereof.

2.0 Objectives

2.1 The main objectives of the Framework are to:

(a) provide an overview of its purpose and components.

(b) outline the manner in which the Framework components come together in an inter-related cohesive manner when providing ISA services.

(c) maintain and continuously improve the quality of ISA.

3.0 Definitions

3.1 **Information Systems Audit (ISA)** is defined as an audit relating to information systems and where applicable, associated systems, with a view to provide independent assurance on the adequacy and effectiveness of information systems controls and processes to manage risks, aligned with enterprise business and governance objectives.

3.2 Brief explanation of the key terms used above is as follows:

3.2.1 **Information Systems (IS)** refers to a set of interrelated components that work together to collect, process, store, and distribute information to support decision-making, coordination, control, analysis, and visualization in an organisation including inter-connected systems, services, and infrastructure utilising a combination of technology, processes, and people to collect, process, store, transmit, and dispose of organisational information. This scope encompasses, but is not limited to, systems supporting Information Technology (IT), operational technology (OT), digital assets, cybersecurity, privacy, and regulatory compliance.

3.2.2 **Information systems risk** is the probability of uncertain events having adverse impact on the achievement of business objectives, related to the vulnerabilities underlying the use, ownership, operation, and adoption of information systems.

3.2.3 **Controls** measures including actions, policies and procedures taken by the organisation to mitigate risks with a view to increase the likelihood that objectives will be achieved.

3.2.4 **Processes** a collection of activities, influenced by policies and procedures, that takes inputs to produce outputs in support of achieving objectives.

3.2.5 **Independent assurance** an objective examination of evidence for purposes of providing a professional assessment on aspects of information systems with the freedom from conditions including influences that may impair professional judgement and may impair the ability to carry out responsibilities in an unbiased manner.

3.2.6 **Governance** the processes and structures implemented by the governing body of an enterprise with a view to inform, direct, manage, and monitor activities toward achieving objectives focused on risk balanced value creation.

3.2.7 **Professional:** A professionally qualified information systems auditor, being a member in good standing of a professional body, such as the ICAI, who undertakes ISA engagements including but not limited to cybersecurity audits and digital personal data protection audits.

4.0 The Framework

4.1 The Framework establishes the structure which governs the domain of ISA. It comprises of the "Definition of Information Systems Audit" (as defined under Para 3.1, above), four key components, and the underlying Code of Ethics. Each of the four components are engrained in the Compendium of Information

Systems Audit Standards inherent to ISA domain. As explained in the Preface, the components are all mandatory in nature, except the Guidance which is recommendatory.

4.2 The four key components (that form the pillars) of the Framework are:

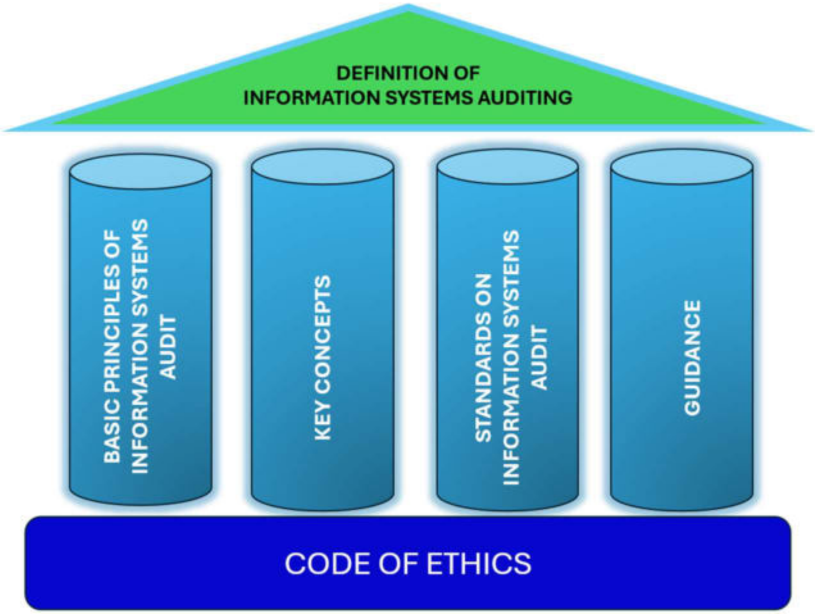
i) Basic Principles of ISA

ii) Key Concepts

iii) Standard on Information Systems Audit

iv) Guidance

4.3 A pictorial depiction of the Framework governing Information Systems Audits is graphically presented below:


DEFINITION OF
INFORMATION SYSTEMS AUDITING
BASIC PRINCIPLES OF INFORMATION SYSTEMS AUDIT
KEY CONCEPTS
STANDARDS ON INFORMATION SYSTEMS AUDIT
GUIDANCE
CODE OF ETHICS

5.0 Code of Ethics

5.1 Every Professional conducting an ISA engagement is bound by a written Code of Ethics (or Conduct), issued by a professional body and/or an organisation of which the Professional is a member. This commits the Professional to the Ethical Standards applied with utmost integrity and sincerity.

5.2 A member of the ICAI, carrying out an ISA engagement is, additionally, governed by the following:

5.2.1. The requirements of the Chartered Accountants Act, 1949.

5.2.2. The Code of Ethics issued by the ICAI, 5.2.3. Other relevant pronouncements of the ICAI.

6.0 Components of the Framework

6.1 Basic Principles of Information Systems Audits

Basic Principles of Information Systems Audits (referred to as the "Basic Principles") are a set of core principles fundamental to the domain of conducting such engagements. The Basic Principles are critical to achieve the desired objectives as set out in the definition of ISA, and therefore, mandatorily apply to all engagements. The basic principles form the essence of the Standards, flow through the standards that in turn support the principles, that enable effective information systems auditing.

Each standard lays down the scope, objectives, requirements, explanatory comments and documentation of work procedures specific to each standard. Together, they help the Professional achieve the purpose of information systems audit.

The basic principles relative to ISAS can be summarised as follows:

6.1.1 Independence

6.1.2 Integrity and Objectivity

6.1.3 Due Professional Care

6.1.4 Confidentiality

6.1.5 Skills and Competence

6.1.6 Principle Aligned Business-IT Context

6.1.7 Systematic Engagement Performance

6.1.8 Effective Communication

6.1.9 Quality and Continuous Improvement

All the nine basic principles are explained in a separate document tilted **Basic Principles of Information Systems Audit.**

6.2 Key Concepts

There are certain concepts which form an integral part of the ISA domain and therefore, apply to most engagements. The key concepts are in the nature of (indicative list):

6.2.1 Nature of Assurance

6.2.2 IS Governance

6.2.3 IS Risk Management

6.2.4 IS Controls

6.2.5 Laws and Regulations

6.3 Information Systems Audit Standards (ISAS)

The Information Systems Audit Standards (ISAS) establish uniform evaluation criteria, methods, processes and practices. The Standards are pronouncements which form the basis for conducting all ISA engagements. These pronouncements are designed to help the Professional to discharge their responsibilities in a consistent and controlled manner.

The Standards are all principle-based, since they define the desired outcome, rather than prescribing a series of procedures or activities to be performed to get to the desired outcome. The Professional is expected to apply best judgement with regard to the procedures and activities required to be conducted to achieve the desired outcome, while factoring in any unusual or unique circumstances.

6.4 Guidance

These are a set of guidelines, which include Guidance Notes, Implementation Guides and Technical Guides. These guidelines are important for implementation of the SIAs and provide clarification for their applicability under particular circumstances.

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

BASIC PRINCIPLES OF INFORMATION SYSTEMS AUDIT

Contents

Paragraph(s)

1.0 Introduction and Scope

1.1 The domain of Information Systems Audit (ISA) bears unique characteristics that have a potential bearing on the achievement of business objectives. The Professionals conducting IS Audits are therefore expected to have certain special attributes and performance requirements. Under the aegis of the Digital Accounting and Assurance Board (DAAB), a non-standing Committee of the Institute of Chartered Accountants of India (ICAI), a set of Information Systems Audit Standards (ISAS or "Standards") are issued to ensure consistency and quality of information systems audits.

1.2 A separate document titled "Framework Governing Information Systems Audits" defines important terms, such as Information Systems Audit, as well as provides an overview of these Standards. In conducting ISA engagements, there are a set of basic principles fundamental to the IS domain covering the credentials of, and work procedures conducted by, the Professional.

1.3 The "Basic Principles" of ISA, as outlined in this document, are critical to achieve the intended objectives in an effective manner. These basic principles form the essence of the Standards, flow through all the Standards that in turn support the principles and enable effective IS auditing.

With these Basic Principles, the Stakeholders at large will have a point of reference to draw up expectations of work undertaken, procedures conducted, record keeping and reporting when conducting ISA engagements.

1.4 **Scope:** All ISA engagements shall be performed based on these basic principles, and departures from these principles shall be appropriately disclosed in any engagement report or other similar communication issued by the Professional.

2.0 Objectives

2.1 The main objectives of the basic principles are to ensure that:

(a) The ISA engagement is undertaken after establishing the credibility of the Professional (see the principles under Para. 3.1 to 3.5).

(b) The ISA engagement is conducted based on certain fundamental tenets that are designed to guide the Professional navigate the special aspects and through the entire lifecycle of the engagement (see the principles under Para. 3.6 to 3.9).

3.0 Basic Principles

3.1 Independence:

The Professional shall be independent and neutral in mind, conduct and appearance. Hence the Professional shall be free from any undue influence which forces deviation from the truth or influences the outcome of the engagement.

For independence, the Professional needs to resist any pressure or interference in establishing the scope of the engagement or the manner in which the work is conducted and reported.

3.2 Integrity and Objectivity:

The Professional shall be honest, truthful, free from bias and uphold the highest standards of integrity. The professional shall act in a highly ethical manner displaying courage across all aspects of the engagement.

The Professional shall avoid all conflicts of interest, bias or fervour and disclose all material facts even in adverse and challenging circumstances. The Professional shall not seek to derive any undue benefits or advantages from their position while upholding the highest standard of legal compliance and ethical behaviour.

3.3 Due Professional Care:

The Professional shall exercise due professional care and diligence while carrying out the engagements. Due professional care is a component of the fundamental principle of "Professional Competence and Due Care," which requires a Professional to act diligently ensuring reasonable care in accordance with applicable technical and professional Standards.

When providing Professional services, due case shall be taken to plan, perform and communicate results, keeping in view the Stakeholders' best interests in context of the engagement objectives and scope.

“Due Professional Care”, however, neither implies nor guarantees infallibility, nor does it require the Professional to go beyond the established scope of the engagement or exceed the brief without due approvals.

3.4 Confidentiality:

The Professional shall at all times, maintain utmost confidentiality of all information acquired during the course of the engagement. This includes the need to protect, among others, proprietary, strategic and operational data and information, personally identifiable information. The Professional shall not disclose any such information to any unauthorised person, while ensuring compliance with applicable laws, regulations, policies, procedures, while using the information for purposes of the engagement.

The information collected or accessed during course of engagement must not be used for personal gain or in any manner prejudicial to the organisation's legitimate and ethical interests and shall ensure due care in protection such information.

3.5 Skills and Competence:

The Professional shall undertake only those engagements for which they have the requisite competence. The Professional shall have the required qualifications and skills and competence to undertake ISA engagements. The Professional shall be either a member of the Institute of Chartered Accountant of India with a post graduate qualification in information systems audit such as the Diploma in Information Systems Audit or a person bearing globally recognised qualifications or certifications in domains such as information technology and systems, cyber security, IT laws and regulations and related domains.

While taking up engagements, the Professional shall ensure having requisite skills and competencies or acquiring necessary skills and competence as part of the audit team, as necessary for the purpose of effectively discharging their responsibilities. The Professional shall also ensure ongoing Continuing Professional Education, skills and expertise including but not limited to domains of technology, legal, operational, strategic and soft skills.

Where the Professional lacks the requisite skills and competence, the Professional may engage in-house or external experts and service providers, who can supplement the Professional team with the required competencies and expertise for effective delivery of the engagement.

3.6 Aligned Business-IT Context:

Information systems need to be aligned with business context to be effective and purposeful, which in turn requires the need for an IS Audit engagement to be similarly aligned to the business and it's IS environment. The Professional shall have a clear understanding of the Business-IT context, given the audit objectives and scope of the engagement. The Professional shall gain a basic understanding of both the explicit and implicit expectations of those charged with governance and other key stakeholders thereby recognising well the purpose of the engagement.

A clear understanding of the Business-IT context is foundational to business risk oriented IS audit and provides the basis for appropriately planning, managing and delivering the engagement and hence enable aligning the engagement objectives with the strategic objectives of the user of IS audit services.

3.7 Systematic Engagement Performance:

The Professional shall understand the IS audit mandate and consider the organisation's governance, risk management, and control processes. Professionals internal to the organisation shall seek to position the IS audit function strategically in order to support the enterprise strategy and goals. Accordingly, the Professional shall put in place and work to an IS Audit plan. IS audit service providers shall plan and perform their engagements strategically aligned with business risk orientation vis-à-vis stakeholders' interests.

The Professional shall establish and conform to methodologies for risk-based planning, human, financial and technology resourcing, co-ordination with internal and external stakeholders and performing IS audit engagements and communicating results of their work in a systematic and disciplined manner with a view to supporting the enterprise objectives of maximising value.

3.8 Effective Communication:

The Professional shall establish and implement robust methodologies and identify all key stakeholders and their interests in focus of the engagement to tailor communications with relevant stakeholders effectively. All IS audit and related communication, including engagement results shall be accurate, objective, clear, concise, constructive, complete, and timely. Effective communication is pivotal to building trust and confidence amongst stakeholders including those in charge of governance and management.

The Professional shall be sensitive to and evaluate the implications of audit observations and recommendations on multiple stakeholders. Where diverse interests may potentially be conflicting in nature, the Professional shall maintain an objective and balanced view. This would enable those in charge of governance to take appropriate measures considering the expectations and interests of stakeholders.

3.9 Quality and Continuous Improvement:

The quality of work performed shall be paramount to the Professional since the credibility of the outcome depends on the reliability of findings. The Professional shall have in place a process of quality control to:

(a) ensure factual authenticity of evidence obtained;

(b) validate the accuracy of all findings; and

(c) continuously improve the quality of the process followed and reports issued.

The Professional shall ensure that an assessment mechanism is in place to monitor performance of the IS audit function and staff members including any external experts. An appropriate peer review mechanism shall be implemented to examine conformance to the applicable pronouncements issued by the ICAI.

4.0 Effective Date

4.1 These Basic Principles are applicable for all engagements beginning on or after XXXXXX

ISAS EXPOSURE DRAFT
(1^{st} Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 110

KEY CONCEPTS

Contents

This Information Systems Audit Standard 110, on "Key Concepts," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or "Standard") deals with certain key concepts which form an integral part of the Information Systems Audit (ISA) domain and therefore, apply to almost all engagements. The key concepts are in the nature of:

1.1.1 Nature of Assurance

1.1.2 Information System (IS) Governance

1.1.3 Information System (IS) Risk Management

1.1.4 Information System (IS) Controls

1.1.5 Laws and Regulations

1.2 **Nature of Assurance:** This requires the Professional to understand the different types of assurance which may be provided. Nature of assurance can vary depending upon the engagement mandate and the type of engagement (refer Para 1.8), and this determination needs to be made prior to acceptance of engagement to help formulate and agree the scope and approach of the engagement.

1.3 **Information Systems Governance (ISG)**: This requires the Professional to understand the various IS governance structures, oversight mechanisms, and operational practices prevailing and to incorporate this understanding in the ISA strategy and approach, as appropriate.

1.4 **Information Systems Risk Management (ISRM):** This requires the Professional to obtain a sufficient understanding of the concept of ISRM framework and practices deployed and to factor these into the ISA strategy, as appropriate.

1.5 **Information Systems Controls (ISC):** This covers the various risk mitigations put in place in the form of IS Controls, which would be the subject of the audit procedures undertaken by the Professional when conducting the engagement.

1.6 **Laws and Regulations:** This deals with the Professional's responsibility to be aware of, and where applicable, comply with the provisions of relevant and applicable laws and regulations governing Information Technology (IT) and related domains (IT Laws and Regulations), relevant to the engagement and where necessary factor such requirements in conducting the engagement.

1.7 **Definitions**: The following terms, along with their definitions, have been used in this Standard.

1.7.1 **Subject Matter** is the matter agreed to be subject to audit and over which the assurance is being sought. It may take various forms such as Information System General Controls, Application Controls, Information System Security Controls, some particular Systems or Process, etc.

1.7.2 **Information Systems Assertion:** An assertion is a claim made by the auditee about the nature of the subject matter. An assertion can be in the nature of Confidentiality, Completeness, Accuracy, Integrity, Availability, Compliances, Efficiency and Effectiveness.

1.7.3 **Suitable Criteria** are the benchmarks or frameworks used to evaluate the subject matter, e.g., Standards of Audit issued by ICAI, ISO Standards issued by International Organisation for Standards, Directions/Guidelines issued by regulator (e.g., Reserve Bank of India).

1.7.4 **Conclusive Outcome:** The outcome of the audit of a subject matter is the conclusion that results from applying the suitable criteria to the subject matter. A conclusive outcome forms the basis of an assurance opinion and is generally in the form of a written report.

1.7.5 **Information Systems Governance (ISG):** ISG encompasses the leadership, organisational structures, and processes which ensure the organisation's technology and information assets support strategic and operational goals. It establishes accountability, decision rights, and performance measurement across the lifecycle of information systems – from planning and acquisition through operation, monitoring, and retirement.

1.7.6 **ISG Framework:** An effective governance framework integrates people, processes, and technology to ensure that technology use is ethical, secure, and contributes to sustainable business outcomes. It promotes transparency, compliance with laws and regulations, and alignment of technology decisions with enterprise risk and performance objectives.

The ISG framework typically includes the following core components:

(a) Strategic alignment between technology and business objectives.
(b) Integration of technology and cyber risks within the organization's overall risk management structure.
(c) Efficient use of resources including personnel, infrastructure, and financial investment.
(d) Performance monitoring using measurable indicators that assess value delivery and resilience.
(e) Clear accountability, roles, and decision-making authority for governance participants.
(f) Promotion of compliance, ethical conduct, and information integrity across all technology activities.
(g) Robust channels and protocols of communication to ensure timely reporting.

ISAS EXPOSURE DRAFT
(1st Dec'25)

1.7.7 **Information Systems (IS) Risk** can be defined as the probability of a threat exploiting vulnerability of Information System (IS) assets or processes or controls by occurrence of an event causing significant impact to the business operations and continuity and which could prevent the organisation from achieving its goals and objectives. IS Risk is termed as Inherent before the application of any mitigation (control) steps, and termed as Residual, post the implementation of mitigation steps.

1.7.8 **Information Systems Risk Management (ISRM)** is the systematic process of identifying, analysing, evaluating, and treating risks related to the use, ownership, operation, and involvement of information and technology assets within the enterprise. ISRM's primary goal is to ensure that information and technology related risks and opportunities to the business are effectively addressed to support the achievement of the enterprise's objectives.

1.7.9 **ISRM Framework** is the combination of structure, systems and processes put in place to organise the various ISRM activities and to integrate them seamlessly into the organisation. The ideal framework includes the following key components:

(a) IS Risk Governance and Strategy: Formal establishment of the mandate, policy, and scope for ISRM. This includes defining risk appetite, roles, responsibilities, and accountability for risk decisions and execution across the enterprise.

(b) Risk Identification and Assessment: The continuous and systematic process for identifying internal and external risk scenarios, determining their potential impact and likelihood, and assessing inherent risk across all IS domains.

(c) Risk Evaluation and Prioritisation: process of comparing assessed risk levels (e.g., High/Medium/Low) against the established risk evaluation criteria and risk appetite to prioritise risks for treatment. This ensures resources are directed to the most critical exposures.

(d) Risk Response and Treatment: The selection and implementation of appropriate actions to mitigate IS risk — such as to tolerate, treat (with controls), transfer or terminate — and the formal documentation of residual risk acceptance by those charged with governance.

(e) Risk Monitoring and Review: The ongoing measurement of the effectiveness of risk responses (especially controls), reporting on risk posture, and performing periodic reviews to ensure the ISRM framework itself remains relevant, effective, and complete in the face of evolving threats and business changes.

1.7.10 **Control Objective:** A Control Objective is a specific, measurable statement that defines the desired purpose or outcome intended to mitigate identified risks and ensure that business operations, financial reporting, and compliance requirements are effectively managed. It establishes the goal or intent behind the design and implementation of one or more controls and provides a basis for evaluating control adequacy and effectiveness.

1.7.11 **Information Systems Controls:** Policies, procedures and technical mechanisms implemented to ensure the confidentiality, integrity and availability of information systems and data.

1.7.12 **Information Security Controls:** Measures designed to safeguard data and protect information systems from unauthorised access, alteration, disclosure or destruction and ensure the reliability and trustworthiness of IS. The measures can take the form of policies, procedures, processes, and technical mechanisms. They are implemented to protect the confidentiality, integrity, and availability (CIA) of information assets – whether stored, processed, or transmitted.

1.7.13 **Cyber Security Controls:** Safeguards implemented to prevent, detect and respond to cyber threats, including malware, ransomware, external intrusions, and other online attacks. These controls are a subset of information security controls specifically designed to protect digital assets, networks, systems, and applications from cyber-attacks and unauthorised intrusions. They include preventive, detective, and corrective measures such as firewalls, intrusion detection systems, endpoint protection, vulnerability management, and incident response processes.

1.7.14 **Data Privacy Controls:** Policies, procedures, and technical safeguards implemented by an organisation to ensure that personal and sensitive information is collected, processed, stored, and shared in compliance with applicable privacy laws and internal policies. These controls are designed to protect individuals' privacy rights and prevent unauthorised access, disclosure, alteration, or misuse of personal data throughout its lifecycle.

1.7.15 **Information Security Control Framework (ISCF)** is the combination of structure, systems and processes put in place to organise the various risk mitigation activities (controls) and to integrate them seamlessly into the organisation as part of the overall IS Risk Management framework.

1.7.16 **IT Laws and Regulations:** Acts or enactments governing and relating to the domains of IS governance and operation (e.g., Information Technology Laws, EU AI Act), underlying Rules to such Acts. Directions and Directives issued by Regulators, Regulatory Advisories and guidelines.

1.7.17 **Compliance Framework:** Compliance framework refers to the whole structure, systems and processes put in place to organise the various compliance activities and to integrate them seamlessly into the organisation.

1.8 **Engagement Mandate and Assurance:** IS audit engagements are driven by the nature of assurance expected or required by the Intended User. Some may require an assurance, while others may not, depending upon the mandate given to the Professional. Hene the audit engagement can be in the form of any one of the following types:

1.3.1 **Assurance Engagement** means an engagement in which the Professional expresses an opinion to give confidence to the Intended Users about the outcome of the audit on the subject matter against a pre-agreed suitable criterion. These engagements can be either of two forms: Reasonable Assurance Engagements, or Limited Assurance Engagements.

1.3.2 **Reasonable Assurance Engagement**- Engagements in which the Professional expresses an audit opinion over the subject matter against the criteria in a positive form, such that Intended User gains confidence over the reliability of the whole subject matter. (e.g., *"Controls over subject matter are designed and operating effectively".*)

1.3.3 **Limited Assurance Engagement** – Engagements in which the Professional expresses an audit opinion over the subject matter against the criterial in a negative form, such that the confidence of the Intended User is limited to only the findings of the audit. (e.g., *"nothing of a material adverse nature came to the attention of the auditor"*).

1.3.4 **Attestation Engagement:** An engagement in which the assurance is in the nature of audit conclusions only (no expression of opinion). Here the Professional validates the assertions (claims) of the auditee and provides a conclusion which expresses whether the auditee assertions are free from material misstatement. (e.g. *"the entity has complied with the Cyber Security Framework issued by the Reserve Bank of India"*).

1.3.5 **Agreed Upon Procedure Engagement**: This is not an assurance engagement since the Professional does not express an audit opinion, but reports the factual findings from the audit procedures conducted over the subject matter which were pre-agreed with the Intended User (e.g., "*Vulnerability Assessment and Penetration Testing (VAPT) engagement"*).

1.3.6 **Non-Assurance Engagement-** All engagements other than those referred above, where in Professional provides advice, consultancy or assistance without expressing any opinion over the subject matter.

1.9 Scope:

1.9.1 This Standards is applicable to the following IS Audit (ISA) engagements:

(a) All engagements that examine IS governance structures, oversight mechanisms, and operational practices related to IS.

(b) An ISA engagement is required to be performed as a part of an External or Statutory Audit.

1.9.2 This Standard is applicable to engagements where:

(a) it is mandated under the provisions of specific IT laws or regulations; or

(b) the Professional is appointed to conduct the ISA as an Auditee requirement which may include (as part of the mandate) an audit of compliance with specified or applicable IT legal and regulatory provisions.

1.9.3 This Standard does not apply to the following engagements listed above (refer Para 1.8):

(a) Agreed Upon Procedure Engagement.

(b) Non-Assurance Engagement.

(c) Where business-technology risk and control orientation is not material to the outcome of the IS audit engagement, regardless of the size or complexity of the enterprise.

1.9.4 Where an IAS engagement may be part of some other larger engagement, such as a Statutory Audit, this Standard is applicable only to the relevant scope of assurance.

2.0 Objectives

2.1 This Standard lays down the following key concepts:

(a) Those relating to nature of assurance engagements and their relevance to the audit procedures to be planned and undertaken by the Professional.

(b) IS Governance framework and mechanisms are designed, implemented and operating effectively to achieve the organisation IS strategy and objectives.

(c) IS Risk Management concepts, especially insofar as it impacts the conduct of IS Audits, and the manner in which the Professional is expected to discharge their responsibilities.

(d) IS Control Framework, and all its applicable elements are adequately evaluated for design and operating effectiveness as part of an IS audit engagement.

(e) Whether the organisation has designed and implemented a formal Compliance framework to ensure that the relevant laws and regulations are complied with when executing the IS activities.

2.2 Some other objectives of the Standard are to ensure that the Professional and (where appropriate) the Intended User:

(a) Have clarity on the nature of assurance the engagement seeks to provide.
(b) Agree that the scope and approach of the engagement is defined appropriately where the assurance is in the form of "expressing an audit opinion".
(c) Incorporate the impact of IS risk and control assessment on the audit engagement planning, performance and reporting.
(d) Recommend improvements to strengthen the IS Governance, Risk and Control environment.

3.0 Requirements

3.1 **Nature of Assurance:** The Professional shall comply with the following when establishing the nature of assurance to be provided as part of the engagement.

3.1.1 Professional shall understand the mandate which is setting the requirements of engagement. Professional shall, in discussion with the Intended User, confirm whether the nature of assurance being sought is in line with this mandate.

3.1.2 Professional shall accept an assurance engagement only where the circumstances indicate that:

(a) The Subject Matter is appropriate.

(b) The Criteria to be used are suitable and agreed with the Intended Users.

(c) A conclusive outcome is achievable, which can form the basis of an assurance opinion. (refer Para 4.1)

3.1.3 Any change in circumstances concerning the nature of the engagement that affects the Intended Users' requirements, shall require a reevaluation of the proposed nature of assurance to be provided as per Para 1.8.

3.1.4 Professional shall, in consultation with the Intended User of Assurance, apply an agreed Suitable Criteria which is appropriate for a reasonable and consistent evaluation or measurement of a subject matter, unless the Suitable Criteria is prescribed by applicable laws or regulatory provisions.

3.1.5 Professional shall consider assertions related to subject matter while conducting the Assurance Engagement.

3.2 **Information Systems Governance (ISG)**: The Professional shall comply with the following which requires an understanding of the implication of ISG as part of developing the scope and approach of the engagement.

3.2.1 Design and structure of ISG Framework: The Professional shall understand whether the organisation's ISG framework is designed and supported with an effective structure. A clear set of requirements shall provide the basis for this evaluation (refer Para 4.2.1).

3.2.2 Strategic Alignment of ISG Framework: The Professional shall consider whether the organisation's ISG framework is appropriately aligned to the overall strategy and business goals of the organisation. A clear set of requirements shall provide the basis for this evaluation (refer Para 4.2.2).

3.2.3 ISG Framework delivers value and governance objectives: The Professional shall understand whether the organisation's ISG framework is designed and implemented to deliver value and mitigate risks of oversight, transparency, and accountability. A clear set of requirements shall provide the basis for this evaluation (refer Para 4.2.3).

3.2.4 ISG Framework aligned to performance management: The Professional shall study whether the organisation's ISG framework adequately supports performance monitoring, measurement, benefit realisation, and continuous improvement. A clear set of requirements shall provide the basis for this evaluation (refer Para 4.2.4).

3.3 **Information Systems Risk Management (ISRM):** The Professional shall comply with the following which requires an understanding of the implication of ISRM as part of developing the scope and approach of the engagement.

3.3.1 Knowledge and Expertise of ISRM: The Professional shall have sufficient knowledge and expertise (or acquire related expertise) of the concept of ISRM Framework and its components, relevant to the nature and scope of the IS audit engagement (refer Para 4.3.1).

3.3.2 Conducting Risk Assessment: The Professional shall, at the time of planning, perform a preliminary assessment of the maturity of the Auditee's ISRM with a view to determine the appropriateness of engagement objectives, scope and execution (refer Para 4.3.2).

3.3.3 Formulating engagement ISRM audit objectives: After performing the preliminary risk assessment that forms part of the engagement planning, the Professional may determine that the ISRM framework maturity is nascent, in which case the engagement scope shall be tailored to evaluate the existence and design of the ISRM framework and its short-comings (refer Para 4.3.3).

3.3.4 Additional audit procedures: Where the Professional, as part of conducting the audit procedures over the existence and design of the ISRM framework, identifies any material deficiencies which have an impact on the Subject Matter of audit, shall incorporate such findings in the performance of any additional work procedures (refer Para 4.3.3).

3.3.5 ISRM Implementation and Effectiveness: Where the preliminary risk assessment indicates that the maturity of the ISRM framework is well designed and in place, the engagement scope shall be tailored to evaluate the level of implementation and the effectiveness of the ISRM to help achieve organisation objectives (refer Para 4.3.3).

3.3.6 Where the objective and scope of the engagement specifically include testing the effectiveness of the ISRM framework, the Professional shall have (or obtain) sufficient ISRM expertise to make an objective assessment of how the framework needs to contribute to help achieve business objectives, in context of the nature and size of the business (refer Para 4.3.4).

3.4 **Information Systems Controls (ISC):** The Professional shall comply with the following which requires an evaluation of the implication of ISC as part of developing the scope and approach of the engagement.

3.4.1 Understanding the Risk and Control environment: The Professional shall obtain a preliminary understanding of the organisation's business structure, regulatory landscape, and key policies to evaluate the overall risk and control environment (refer Para 4.4.1).

3.4.2 Control Objective: As part of the preliminary risk assessment undertaken by the Professional (refer Para 3.2.2), the Professional shall identify key controls relevant to the audit engagement. Understanding the respective control objectives of these key controls shall be used to formulate the engagement objectives (refer Para 4.4.2).

3.4.3 Control design effectiveness: When developing the audit strategy, the Professional shall undertake an assessment of the manner in which the IS Control has been designed and incorporated into the information systems and processes to mitigate the related risk (refer Para 4.4.3).

3.4.4 Operating effectiveness: When developing the audit strategy, the Professional shall undertake an assessment of how well a control is actually functioning in practice and thereby, helps to achieve the intended control objective (refer Para 4.4.4).

3.5 **Laws and Regulations (L&R):** The Professional shall comply with the following which requires an evaluation of the implication of L&R as part of developing the scope and approach of the engagement.

3.5.1 Knowledge of IT laws and Regulations: The Professional shall possess, or acquire through an expert, adequate working knowledge and understanding of the applicable IT laws and regulations especially those relevant to the scope and objectives of the engagement (refer Para 4.5.1).

3.5.2 Assessment of Compliance framework: The Professional shall undertake an understanding of the IT Compliance framework put in place by the organisation to ensure its compliance with the relevant IT laws and regulations. This understanding shall extend to a review of the design and operating effectiveness of those laws and regulations which are considered high risk and entail high penalties of non-compliance on the organisation (refer Para 4.5.2).

3.5.3 Formulating audit Plans: The Professional shall factor the requirements of the relevant provisions of applicable IT laws and regulations, in planning the engagement and in design of work programs. This may include assessing the need for necessary legal and regulatory expertise and, if necessary, engaging external domain experts (refer Para 4.5.3).

3.5.4 Reporting Compliance deviations: The Professional shall identify and report any significant deviations or non-compliances concerning IT laws and regulations impacting the subject matter of the engagement (refer Para 4.5.4).

3.5.5 Information Management: Professional shall obtain, use, retain and disclose the necessary information required for and related to audit in accordance with the provisions of laws and regulations (refer Para 4.5.5).

4.0 Explanatory Comments

4.1. **<u>Nature of Assurance (refer Para 3.1.2):</u>** The following are the three components which make an engagement an assurance engagement:

1. Three Party Relationship:
   (a) The Professional;
   (b) The Auditee; and
   (c) The Intended User of the assurance.
2. Three key Elements:
   (a) An Appropriate Subject Matter;
   (b) Suitable Criteria; and
   (c) Conclusive Outcome.
3. A written Assurance report which expresses an Audit Opinion.

4.2. **<u>Information Systems Governance (refer Para 3.2):</u>** The following provides further explanations to the requirements:

4.2.1 <u>Design and structure of ISG Framework (refer Para 3.2.1):</u> The following requirements can provide the basis for understanding whether the ISG framework is designed effectively:

(a) existence of board-level oversight for technology investments and risk management.
(b) effectiveness of governance committees or steering groups that oversee technology initiatives.
(c) roles, responsibilities, and authorities are clearly defined, communicated and enforced.
(d) segregation between governance, management, and operational responsibilities.
(e) ISG structure enables strategic responsiveness while maintaining control, and the deployment of technology is purposeful, compliant, and value-oriented.
(f) adequacy and enforcement of technology governance policies and procedures.

4.2.2 <u>Strategic Alignment of ISG Framework (refer Para 3.2.2):</u> The following requirements can provide the basis to consider whether the ISG framework is strategically aligned:

(a) existence of a documented technology strategy aligned with organizational goals.

(b) translation of strategic objectives into actionable technology initiatives and investments.

(c) technology leadership participates in strategic planning and budgeting.

4.2.3 <u>ISG Framework delivers value and governance objectives (refer Para 3.2.3):</u> The following requirements can provide the basis for understanding whether the ISG framework delivers value and governance objectives:

(a) processes used to prioritize and approve technology investments are based on expected business value.

(b) realized benefits are measured and reported after project completion.

(c) service delivery quality, customer satisfaction, and value tracking mechanisms are in place.

4.2.4 <u>ISG Framework aligned to performance management (refer Para 3.2.4):</u> The following requirements can provide the basis for evaluating whether the ISG framework adequately covers performance management:

(a) performance indicators and reporting metrics are clearly defined and aligned with objectives.

(b) management and the Board receive periodic performance reports and take corrective actions.

(c) realised benefits are measured and reported after project completion.

(d) continuous improvement mechanisms are in place to enhance governance effectiveness.

4.3. **<u>Information Systems Risk Management (ISRM) (refer Para 3.3):</u>** The following provides further explanations to the requirements:

4.3.1 <u>Knowledge and Expertise of ISRM (refer Para 3.3.1):</u> The Professional shall have (or acquire) adequate understanding of the fundamental concepts of IS Risks and ISRM frameworks (refer Para 1.7) and how these are relevant and applicable to the proper conduct of IS Audits. The Professional shall ensure the availability of requisite competence and skills in independent assessment of the design and operating effectiveness of the ISRM framework.

Where the ISRM framework, and its various elements are large and complex in nature (e.g., due to nature of business or due to emerging technologies), the Professional may consider using the help of an expert in the area, as per ISAS 220 which covers "Using the work of an Expert".

4.3.2 <u>Conducting Risk Assessment (refer Para 3.3.2):</u> As part of engagement planning, the Professional shall undertake a preliminary risk assessment in line with ISAS 220 covering "Engagement Planning". The outcome of this exercise will allow the Professional to make a determination of the maturity level of the prevailing ISRM framework, i.e., to what extent a formal ISRM framework has been developed and implemented (or adopted from other sources, e.g., ISO Standard on Information Technology or Risk Management).

Where the Professional is undertaking an examination of an organisation which is small in operations, or a business not highly automated or technology dependant, the Professional may not find formal documentation of risks and controls, and the preliminary risk assessment shall be informal in nature and directed to assess if the basic objectives of ISRM are achievable in context of the size and nature of the organisation.

4.3.3 Formulating engagement ISRM audit objectives (refer Para 3.3.3 to 3.3.5): Where the objectives and scope of engagement require an audit of ISRM, the Professional shall, after conducting a preliminary risk assessment, makes a determination of the following:

(a) Whether the ISRM framework is in existence (informally in practice, for small organisations or formally in documented form, for large organisations).

(b) If ISRM framework is in existence, to what extent it has been adopted and fully implemented in practice.

(c) If implemented, what is the maturity level of implementation and whether it is operating in practice.

(d) The outcome of this preliminary assessment will help to formulate the engagement objectives of audit testing for ISRM design and operating effectiveness.

4.3.4 The effectiveness of ISRM is of critical concern to the Professional, as it directly impacts the control environment, reliability of controls and hence the quality of audit. The relevance of ISRM varies significantly across organisations, influencing the specific evidence the Professional seeks.

4.4. **Information Systems Controls (ISC) (refer Para 3.4):** The following provides further explanations to the requirements:

4.4.1 Understanding the Risk and Control environment (refer Para 3.4.1): This understanding of the relevant risks and controls provides the necessary context for assessing governance mechanisms, risk management practices, and the internal controls operating within the organisation.

The Professional shall possess the competence (or acquire the expertise) to understand the complexities of existing and emerging technologies to identify associated risks and evaluate the adequacy of controls within the scoped audit area. This includes the ability to interpret technology architectures, assess control design, and determine the impact of evolving digital environments on the organization's risk profile.

4.4.2 Control Objective (refer Para 3.4.2): These establish the goal or intent behind the design and implementation of one or more controls and provides a basis for evaluating control adequacy and effectiveness.

Key characteristics of control objective are in the nature of:

(a) Aligned with risks: Each control objective corresponds to one or more identified risks.

(b) Measurable: Enables assessment of whether the control has achieved its intended purpose.

(c) Action-Oriented: Describes what the control should accomplish, not how it is implemented.

(d) Supports Assurance: Forms the foundation for designing audit procedures and evaluating control performance.

4.4.3 Control design effectiveness (refer Para 3.4.3): This refers to the degree to which a control, if implemented and performed as intended, is capable of preventing or detecting material errors, fraud, or non-compliance in a timely manner. It evaluates whether the control is properly designed to address the identified risk. It evaluates the structure, logic, and adequacy of a control – not whether it is actually operating. Assessing control design effectiveness gives an assurance that structure, logic and adequacy of a control in achieving the overall control objective.

4.4.4 Operating effectiveness (refer Para 3.4.4): This refers to how well a control is operating in practice - that is, whether it functions as designed, consistently over a defined period of time. It evaluates whether the control is working effectively and reliably to prevent or detect errors and irregularities.

4.5. **Laws and Regulations (L&R) (refer Para 3.5):** The following provides further explanations to the requirements:

4.5.1 Knowledge of IT laws and Regulations (refer Para 3.5.1): Where the appointment of the Professional is under any specific IT law or regulation, the Professional shall formulate the objectives and scope of the engagement in line with the relevant provisions of such IT laws and regulations.

(a) Where the appointment of the Professional is not under any specific IT law or regulation, the Professional shall formulate the objectives and scope of the engagement to undertake as assessment whether the organisation is materially in compliance with the relevant provisions of IT laws and regulations.

(b) This determination is made at the time of acceptance of engagement and by assessing the available competence and skills in the audit team. At the engagement acceptance stage, the Professional shall inquire with the Auditee Management and obtain written representation if required about the applicable laws and regulations.

4.5.2 Assessment of Compliance framework (refer Para 3.5.2): As the prime responsibility of compliance rests with management, the Professional shall undertake a study of the compliance farmwork put in place to help the organisation monitor and track its compliance obligations. Where the laws and regulations are considered high risk and could result in large penalties on the organisation for non-compliance, the Professional shall extend the audit procedures to assess the design and operating effectiveness of the Compliance framework.

4.5.3 Formulating audit Plans (refer Para 3.5.3): The Professional shall integrate IT legal and regulatory compliance considerations into engagement planning, encourage multidisciplinary collaboration and, if necessary, engage an expert where specialized interpretation or domain expertise is required.

4.5.4 Reporting Compliance deviations (refer Para 3.5.4): As a result of conducting work procedures designed to identify and evaluate any material deviations or breaches of applicable IT laws or regulations affecting engagement objectives or audit subject matter, any such material compliance deviations shall be included in the audit findings and reported accordingly.

4.5.5 Information Management (refer para 3.5.5): The Professional shall put in place a robust process for lawful handling of audit information covering collection, use, retention, and disclosure, in strict conformity with statutory and regulatory provisions governing confidentiality and data protection, where so required by such laws or regulation.

5.0 Documentation of Work Procedures

An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.1 **Nature of Assurance:**

(a) An Appointment Letter from Auditee describing the Nature of Assurance and expectations of Intended Users.

(b) Engagement Letter issued by the Professional.

(c) Communication regarding clarity of scope, subject matter, suitable criteria etc.

(d) Documentation confirming the agreed nature of assurance.

5.2 **IS Governance:**

(a) General: governance documentation, policies, and strategy papers.

(b) Interviews: Discussions with key governance stakeholders to validate design and operational effectiveness of governance mechanisms.

(c) Evidence Evaluation: Summary of management assertions.

(d) Reporting: Summarising findings, risk implications, etc.

5.3 **IS Risk Management:**

(a) Documentation of process for preliminary assessment of state of ISRM and its impact on the engagement objectives and scope.

(b) Records of communication with Auditee on obtaining preliminary information on ISRM Framework, its components and considerations critical to the planning and performance of the engagement.

(c) Documentation of assessment of any material deficiencies in ISRM and its impact on the objectives and scope of the engagement, nature, timing and extent of audit procedures.

(d) Specialised ISRM Audit Plan (Where applicable): Where the audit specifically includes an examination of the ISRM framework, the documentation of the expert knowledge applied and the specific methodology used. This includes documenting the tests performed, the criteria used, and the findings to evaluate the effectiveness of ISRM's functioning.

(e) Summary of material deficiencies and control weaknesses identified within the ISRM framework, stating the root cause and the impact of these weaknesses on the subject matter of audit. A communication log can be maintained, detailing when and to whom these findings were formally reported.

5.4 **IS Controls:**

(a) Planning process documentation (or checklists) and any tools used in the planning process.

(b) Documentation supporting the information gathered about the business and operations, systems and processes and any past or known issues.

(c) Summary of meetings and communication with key Stakeholders, with a summary of their inputs.

(d) Summary of resource requirements and comparison with available resources, competencies and matching of skills with the assignment requirements.

5.5 **Laws and Regulations:**

(a) The engagement planning memorandum documents applicable IT laws, scope alignment, relevant regulations, and assessment of professional competence before accepting the engagement.

(b) A legal and regulatory mapping sheet lists statutory provisions, compliance obligations, and control areas applicable to the engagement for reference during planning and testing.

(c) Compliance testing workpapers showing procedures performed, evidence obtained, exceptions identified, and conclusions on adherence to specific legal and regulatory requirements.

(d) An expert consultation log captures the need for legal or regulatory expertise, minutes of meetings, inputs and opinions received, and their influence on audit conclusions and recommendations.

(e) The compliance summary and reporting file consolidates identified non-compliances, their legal implications, management responses, and final communication to stakeholders or regulators.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 210

BUSINESS AND INFORMATION SYSTEMS CONTEXT

Contents

Paragraph(s)

This Information Systems Audit Standard 210, on "Business and Information Systems Context," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or "Standard") emphasises the importance of understanding the business dynamics and the prevalent information systems and how the two relate to each other (the context), an exercise which needs to be conducted prior to the commencement of the Information Systems (IS) audit engagement.

1.2 **Definitions**: The following terms, along with their definitions, have been used in this Standard.

1.2.1 **Information Systems (IS) Universe:** The complete and comprehensive inventory of all technology components, processes, systems, applications, infrastructure, and associated human and other resources and third-party services that are owned, managed, or utilised by an organisation to achieve its business objectives.

1.2.2 **IS Audit Universe:** The complete and comprehensive inventory of all auditable IS technologies, processes, systems, applications, infrastructure, projects, and organisational units within an enterprise. It represents the entire population of potential IS areas that could be subject to an IS audit engagement.

1.2.3 **Business Technology Alignment:** The process of ensuring that an organisation's information technology strategies, resources, and operations are closely integrated with its overall business goals and objectives. This alignment enables IS initiatives to directly drive, support and enhance business performance, improve efficiency, and inspire value creation by fostering collaboration between IS and business stakeholders for enterprise value maximisation.

1.3 **Scope:** This standard applies to all types of IS audit engagements undertaken by the Professional.

2.0 Objectives

2.1 The primary objective of this Standard is to ensure that the Professional gains requisite understanding of the business, strategic, regulatory, operational, and technological landscape of the auditee organisation, and appropriately factors such understanding across the various phases of an IS audit engagement.

2.2 Other objectives of this Standard are as follows:

(a) To identify and understand the critical business functions and their reliance on IS for assessing relative Business IS Risk and accordingly plan the engagement.

(b) Identify and understand the complexity of the IS Universe and assess the need for designing work procedures and applying automated audit tools and techniques, or for engaging experts, if required.

(c) Optimise the results of the IS audit engagement particularly for those in charge of governance and business management.

3.0 Requirements

3.1 **Business Dynamics:** The Professional shall obtain requisite and formal understanding of the business dynamics including but not limited to nature, size, constitution, organisation and complexity of the business and profile of business transactions of the industry vertical in which the organisation operates, key external and internal factors, relevant to the engagement objectives and scope (refer Para 4.1).

3.2 **Prevalent Information Systems Universe:** The Professional shall obtain requisite and formal understanding of the prevalent IS Universe and the level of automation of various business and supporting processes, which include but not limited to, IS components including business applications, technology components, associated processes, services including third party services and people, relevant to the engagement objectives and scope (refer Para 4.2).

3.3 **Evaluating the Combined Context:** The Professional shall obtain requisite understanding of the combined context of the business and IS, their alignment, their interactions and dependencies and the impact of IS on the achievement of the business and operational objectives of the organisation (refer Para 4.3).

3.4 **Refining Audit Strategy and Objectives:** Based on such understanding of Business and IS Context, the Professional shall confirm or propose modifications to the objectives and scope of the engagement, as necessary. (refer Para 4.4)

4.0 Explanatory Comments

4.1 **Business Dynamics (refer Para 3.1):** The dynamics of any business are fluid, but would comprise of the following:

(a) Structure: legal entity, pattern of ownership and governance structure, internal and external stakeholders.

(b) Strategy & objectives: organization's strategy and objectives and related business risks.

(c) Sectoral context: Industry sector, its unique aspects and related regulatory challenges.

(d) Geographic Presence: Spread of the business across geographic regions and location specific regulatory obligations.

(e) Business Operations: Key business functions, target customer categories, critical resources, internal & external dependencies and key contractual obligations.

(f) Change Drivers: Recent or ongoing merger, acquisitions, business transformation initiatives, and any other significant changes since last such similar audit engagement.

4.2 **Prevalent Information Systems Universe (refer Para 3.2):** The IS Universe is ever changing, but would comprise of the following information:

(a) IS Landscape: Inventory of various information systems, applications, platforms, databases, infrastructure, interfaces and the inter-dependencies between these components.

(b) IS Architecture and Flow: The architecture of information systems and flow of data and information across layers of internal and external information systems, applications, business processes in the form of Data / Information flow diagrams.

(c) Data, System, Infrastructure Architecture: Identification and classification of Data, Information and other information assets, Identity access control practices, identify change control practices, internal and external system boundaries and Tools and technologies used to secure the information assets.

(d) Entity Level Controls and Control Environment: Presence of tone at the top, culture, values and ethical behaviour, presence and effectiveness of information systems aligned with and governed by entity level controls.

4.3 **Evaluating the Combined Context (refer para 3.3):** The Professional's understanding of the combined Business and IS Context helps in confirming the engagement objectives set by the management and the scope of the engagement. Professional shall engage with the relevant business stakeholders, to gather contextual insights and to validate their understanding of the IS Universe and its alignment with the business objectives keeping in mind the size, nature and complexity of the organisation, business environment and the IS eco-system.

4.4 **Refining Audit Strategy and Objectives (refer Para 3.4):** The Professional's understanding of the business and information systems context, is significantly relevant in ensuring the Professional is aligned with the Auditee's expectations from the engagement. This especially includes the expectations of those charged with governance. Where the Professional, based on such understanding, determines a need to modify the scope of the engagement or its objectives, the criteria, they shall propose necessary modifications to the scope or objectives of the engagement, as appropriate.

The Professional shall appropriately utilise the results of the Business and IS Context across the stages of engagement planning, risk assessment, engagement resource management including need for engaging external experts, design of work procedures, performance and communication of audit results.

5.0 Documentation of Work Procedures

An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.1 Gaining understanding: Methodology followed by the Professional in gaining formal understanding of the Business and IS Universe Context.

5.2 Business Context Profile: Document the entity's nature, industry, complexity, and key internal/external factors relevant to the engagement scope.

5.3 IT Universe Inventory and Automation: List all key applications and underlying business processes and extent of automation, technology components, third party dependencies, services.

5.4 Alignment and Dependencies: Document information systems' impact and dependencies on achieving the organization’s core business and operational objectives.

5.5 Scope Rationale: Justify and document the final decision to confirm or modify the engagement objectives, subject matter, and scope.

5.6 Risk and Resource Allocation Record: Document how context analysis determined engagement risks, resource needs, and the requirement for external expertise.

5.7 Procedure Design Linkage: Document the clear link between the understanding of business context and the design of specific audit work procedures and steps.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1^{st} Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 220

ENGAGEMENT PLANNING

Contents

Paragraph(s)

This Information Systems Audit Standard 220, on "Engagement Planning," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

ISAS EXPOSURE DRAFT (1st Dec'25)

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or "Standard") covers the essential planning steps required to plan and conduct an Information Systems (IS) Audit. In certain engagements, where there is a need to engage the services of an Expert, this Standard sets out the principles governing the selection, engagement, supervision, and evaluation of the work of the Expert. Finally, the Standard also deals with the responsibility of the Professional to have an effective communication and interaction with its stakeholders.

1.2 Information Systems Audit (ISA) Planning is undertaken at two levels:

(a) An overall ISA plan is prepared for the entire entity covering multiple auditable units to be completed over a given period of time (usually a year). This entity level ISA plan is presented for approval to the highest governing body responsible for IS audits, generally the Audit Committee of the Board, or in some cases to the Chief of Internal Audit.

(b) The entity level ISA plan is divided into multiple smaller ISA assignments covering some part of the entity, such as an area, activity or process. Before the IS audit of any auditable unit can be undertaken, a specific ISA plan is prepared for each respective assignment.

This Standard covers the first level of planning for the entity as a whole. IS Audit Standard (ISAS) 310, covers the detailed planning undertaken when executing an assignment for a particular auditable unit covering some part of the entity.

1.3 **Definitions**: The following terms, along with their definitions, have been used in this Standard.

1.3.1 **Mandate:** The source of authority under which the IS audit engagement is undertaken, clarifying the expectations, and which may arise from laws, regulations, those charged with governance (e.g., Board of Directors, executive management), or other competent authorities or bodies.

1.3.2 **Engagement:** An Engagement shall mean the overall official mandate agreed between the Professional and the Primary Stakeholder, stipulating the terms of reference, scope of work, coverage, and expected deliverables. It generally encompasses multiple auditable units and the arrangement is contracted in the form of either an Engagement letter (in case of an external service provider) or documented in the form of an Audit Charter (in the case of an in-house audit function).

1.3.3 **Assignment:** An Assignment shall mean some part of the engagement covering a distinct auditable unit (such as a specific business location), or a portion of the overall business activity (such as IT application controls) or a specific group of tasks (such as Penetration Testing).

1.3.4 **Expert:** An Expert is a person or entity possessing specialised technical competence, professional experience and recognised credentials in one or more domains of IS including but not limited to cyber security, data analytics, cloud and network architecture, digital forensics or operational technology expertise, which is necessary to achieve the objectives of the IS audit engagement.

1.3.5 **Communication:** Communication refers to sharing of any information or data between the Professional and the Stakeholders, in any form (e.g., verbal, written, electronic/digital, etc.) or format (e.g., documents, images, videos, text messages, etc.) or any other interaction (e.g., physical or electronic meetings).

1.3.6 **Stakeholders:** A general term which shall refer to both the primary stakeholders as well as other stakeholders, as defined herein.

1.3.7 **Primary Stakeholder:** Primary Stakeholders are those charged with Governance, especially those charged with IS Governance (e.g., Board of Directors, Audit Committee, etc.) and may include executive management of the organisation (e.g., Chief Technology Officer, etc.). Those who have the responsibility to appoint the Auditor and oversee the performance and accountability of the auditee may also be considered as the Primary Stakeholder.

1.3.8 **Other Stakeholders:** All Stakeholders other than the Primary Stakeholders are considered as Other Stakeholders and include third parties (e.g., company officials and staff, the users of the audit report, government bodies and regulators, experts hired by the organisation, third-party service providers, business associates, etc.).

1.4 **Scope:** This standard applies to all engagements related to IS audits undertaken by the Professional.

1.4.1 Where some part of the engagement is outsourced to the Professional as an assignment, this Standard shall apply only to the extent the Professional needs to plan the activities of the outsourced part of the assignment. In some situations, such as where the small size and simple nature of the entity's business may not justify multiple audits, the engagement and assignment could be one and the same

1.4.2 This Standard shall also apply to all IS Audit engagements where the Professional engages, relies upon or makes use of the work of an Expert for performing specialised audit procedures, evaluating technical evidence, or forming audit conclusions.

1.4.3 Communication of audit observations and findings through audit and other reports is out of the scope of this standard, since this is covered under ISAS 510 on "Reporting Results".

2.0 Objectives

2.1 The Primary objectives of this Standard are to ensure that the Professional completes the overall ISA engagement planning with all the essential steps required to achieve the engagement mandate and objectives as agreed with the Primary Stakeholder.

It expects the professional to:

(a) understand the broad mandate and objectives of the ISA engagement, and formally agrees the same with the Primary Stakeholder.

(b) Gain the requisite understanding of the business, strategic, regulatory, operational, and technological landscape of the organisation, and appropriately factors such understanding across the various phases of an IS audit engagement. This includes factoring in the requirements of ISAS 210 on "Business and IS context:".

(c) Provide a uniform approach for identifying, evaluating, engaging, and supervising the work of an Expert so that such work contributes meaningfully to the audit outcome.

(d) Emphasise the need for an ongoing interaction and an exchange of important information between the Professional and the Stakeholders across the duration of an engagement with a view to improve the overall quality of the audit output.

2.2 The achievement of the overall objectives is supported by the following specific objectives:

(a) Confirm and agree with the Primary Stakeholder the broad scope, methodology and depth of coverage of the IS audits to be undertaken.

(b) Identify and understand the critical business functions and their reliance on Information Systems for assessing relative Business IS Risk and accordingly plan the engagement.

(c) Study the entity's risk assessment and risk mitigation activities to adequately incorporate the same as part of the audit plan.

(d) Identify and understand the complexity of the IS Universe and assess the need for designing work procedures and applying automated audit tools and techniques, or for engaging experts, if required.

(e) Evaluate the adequacy of overall audit resources, their skill and competence and that they are deployed well, with proper focus in areas of importance, complexity and sensitivity.

(f) Ensure that the audit procedures planned to be undertaken conform with the applicable laws, regulations, and pronouncements issued in the IS and audit domains.

3.0 Requirements

3.1 **Engagement Mandate and Objectives:** The following provides a summary of the key requirements:

3.1.1 The Professional shall seek inputs from the Primary stakeholder and get confirmation in writing the understanding reached as to the nature of the engagement mandate and audit assurance (refer para 4.1.1).

3.1.2 The Professional shall, based on the agreed mandate and expected audit assurance, formulate the detail engagement objectives and goals. These would be shared with key Stakeholders to seek clarity and confirmation so that they can form the basis of engagement planning (refer Para 4.1.2)

3.2 **Process driven Planning Exercise:** The following provides a summary of the key requirements:

3.2.1 The Professional shall undertake a process driven planning exercise, the outcome of which shall be a written IS Audit engagement plan containing the following essential elements (refer Para 4.2.1):

(a) Knowledge of business and supporting IS environment (refer Para 4.2.2)

(b) Understand the entity level IS risk environment and mitigation activities (refer Para 4.2.3)

(c) Discussion and dialogue with key stakeholders (refer Para 4.3.4)

(d) Requirement and availability of engagement resources and their competence (refer Para 4.3.5)

3.2.2 The Professional shall ensure that the audit engagement undertaken conforms with the applicable laws, regulations, and pronouncements issued in the IS and audit domains.

3.3 **Using the work of an Expert:** The following provides a summary of the key requirements:

3.3.1 The Professional shall determine the need to engage an Expert having regard to the nature, complexity, and criticality of the IS environment, the scope and objectives of the audit, the competence available within the team, and any statutory or contractual requirement mandating expert involvement (refer Para 4.3.1).

3.3.2 Where specialised technical knowledge or skills are required for performing audit procedures, evaluating system controls, or interpreting complex results, the Professional shall identify, evaluate, and engage an Expert after assessing:

(a) The independence and objectivity of the Expert, including any association with the auditee or its service providers (refer Para 4.3.2).

(b) The competence and capability of the Expert, considering qualifications, certifications, experience, and domain knowledge (refer Para 4.3.3); and

(c) The methodology, tools, and procedures proposed by the Expert, together with their ability to comply with confidentiality and data-protection obligations. (refer Para 4.3.3 & 4.3.4)

3.3.3 The engagement shall be governed by written terms clearly defining the scope of work, deliverables, responsibilities, reporting format, confidentiality provisions, timelines, and limitations of liability, and shall be integrated within the overall audit plan under the Professional's direction and supervision (refer Para 4.3.4).

3.3.4 The Professional shall review and evaluate the Expert's work to confirm that it has been performed in accordance with the agreed scope, that the results are technically sound and supported by evidence, and that any limitations or deviations have been explained and resolved (refer Para 4.3.5).

3.3.5 The Professional shall evaluate whether the Expert's work is to be referenced in the audit report or incorporated as part of it, but shall retain overall responsibility for the conduct of the engagement and the conclusions expressed, irrespective of the extent of reliance placed on the Expert (refer Para 4.3.6)

3.4 **Communication with Stakeholders:** The following provides a summary of the key requirements:

3.4.1 Communication with Stakeholders concerning all matters of the engagement shall be in accordance with a laid-down process and a pre-defined, pre-agreed protocol, channels of communications, frequency which shall clarify the responsibility of the Professional to communicate directly with Primary and Other Stakeholders on matters relating to the engagement. (refer Para 4.4.1)

3.4.2 The Professional shall establish an Escalation Protocol for certain unexpected situations during the performance of audit engagement, which may hinder the timely completion of the engagement and which should incorporate the intervention of Primary Stakeholder at an appropriate time.

3.4.3 The form and content of matters to be communicated and the timeframe of communication are based on the best judgment of the Professional unless the law, regulation or auditee policy provides for any specific form and content.

3.4.4 The Professional shall exercise good communication etiquettes at all times and ensure that the communication is on-going, accurate, complete and timely. The Professional shall communicate certain matters considered to be as "Essential Matters" and certain matters considered to be as "Significant Matters." (refer Para 4.4.2 and 4.4.3)

3.4.5 The Professional shall not disclose or divulge any information obtained during the engagement without the prior express permission of the Primary Stakeholders or unless otherwise required by any law.

3.4.6 Communication with Other Stakeholders shall be pre-defined and duly included in the process and protocol. The consent (and if necessary) the prior approval the of Primary Stakeholder is essential for any communication with Other Stakeholder. Communication with Other Stakeholder may set through Primary Stakeholder rather than the Direct Communication.

3.4.7 Professional may establish key performance measures to monitor the effectiveness of communication as part of Quality Assessment and Improvements.

4.0 Explanatory Comments

4.1 **Engagement Mandate and Objectives (refer Para 3.1):** The following provides further explanations to the requirements:

4.1.1 Establishing Engagement Mandate: The Professional shall, ideally before appointment, but certainly before IS Audit planning, undertake a dialogue with the Primary Stakeholder to discuss the details of the mandate and, if relevant, the source of the mandate, such as the relevant laws, regulations etc. The mandate in some respects will drive the nature of assurance which may be excepted under the circumstances. The Professional shall be guided by ISAS 110 which covers "Nature of Assurance" to gain an understanding with the Stakeholder on the type of audit assurance which can be provided. This understanding shall be documented in writing as part of an Engagement Letter or an Appointment agreement.

4.1.2 Formulating Engagement Objectives: Based on the mandate agreed with the Primary Stakeholder, the Professional shall formulate this into broad high-level IS Audit engagement objectives, scope and approach. For example, if the agreed mandate of the IS Audit is not just to evaluate the design and effectiveness of the IS control environment, but extends to also improve the same, then the objectives and scope of the engagement will be expanded to accommodate the larger mandate.

4.2 **Process driven Planning Exercise (refer Para 3.2):** The following provides further explanations to the requirements:

4.2.1 Planning process: The Professional shall apply a laid down planning process to be followed in completing all essential planning activities. This process shall stipulate the essential inputs, steps required to complete the planning activities and the nature of output required to conduct a comprehensive planning exercise.

4.2.2 Knowledge of Business and IS environment: The Professional shall undertake an understanding of the nature of the entity's business and IS environment and how the two are supporting the achievement business objectives and goals. Also refer to ISAS 210 on "Business and Information Systems Context" to arrive at conclusions required to formulate the detailed engagement plans.

4.2.3 Understanding entity level IS risk environment: The Professional shall review the IS risk assessment documentation of management to gain the required knowledge and appreciation of the challenges faced by the entity in achieving key business objectives. In addition, the Professional shall undertake an independent high level IS risk assessment relevant to the Audit Universe and the main auditable units to validate their importance and audit priority. The Professional will be guided by ISAS 110 which covers "IS Risk Management" to formulate the detailed engagement plans.

4.2.4 Discussion with Stakeholders: The Professional shall engage in extensive discussions and dialogues with all key Stakeholders, including executive and IS management, process owners, statutory auditors etc. Their inputs shall be used as a sound basis to understand the intricacies of engagement requirements and help identify important matters for consideration and also to align stakeholder expectations with audit objectives.

4.2.5 Resource Assessment and Allocation: The Professional shall undertake an exercise to evaluate the required number of resource and competencies (knowledge, experience, expertise, etc.), and based on prevailing availability of resources, make a determination of:

(a) Any critical skills/expertise gaps in the audit team.
(b) Plans to close any resource gaps by acquiring additional resources.
(c) Consider engaging the services of external experts.

4.3 **Using the work of an Expert (refer para 3.3):** The following provides further explanations to the requirements:

4.3.1 Determinants for engaging an Expert: The Professional shall consider the engagement of an Expert when the complexity, size, or risk of the information systems environment requires specialist technical input. The decision shall be based on business relevance, system criticality, and the need to enhance the reliability of audit findings.

4.3.2 Independence and objectivity: The Professional shall ensure that the Expert engaged is independent of the auditee and free from any relationship that may impair objectivity:

(a) The Expert shall not have been involved in the design, implementation, or management of the system under audit.

(b) Any association or interest with the auditee or its technology service providers shall be disclosed and evaluated.

(c) Where the Expert is an internal employee of the auditee, written safeguards and independence confirmations shall be obtained.

4.3.3 Competence and methodology: The Professional shall evaluate the Expert's competence, domain experience, and use of sound methodologies consistent with the audit objectives:

(a) The Expert shall communicate the approach, tools, and control mechanisms proposed for execution.

(b) The Professional may compare the adequacy of such methods with recognised industry or regulatory practices before confirming engagement.

4.3.4 Confidentiality and data-protection compliance: The Expert shall operate under the same confidentiality and data-protection obligations as the Professional. Access to system data, logs, or other sensitive digital artefacts shall conform to applicable legal, contractual, and organisational requirements. The terms of engagement shall specify responsibilities for data handling, evidence retention, and secure destruction.

4.3.5 Integration and supervision of Expert work: The Professional shall integrate the Expert's work within the overall audit plan and exercise direction and supervision throughout the engagement. Communication between the audit team and the Expert shall be maintained to ensure clarity on scope, deliverables, and reporting timelines. Where the Expert's work forms part of the audit report, the Professional shall review the content for technical soundness, and completeness.

4.3.6 Evaluation and documentation: The Professional shall evaluate whether the Expert's work has been carried out in accordance with the agreed scope and whether conclusions are supported by adequate technical evidence. Any limitation or deviation identified shall be recorded along with compensating procedures undertaken, and the evaluation shall be documented as part of the working papers supporting the final audit conclusion.

4.4 **Communication with Stakeholders (refer Para 3.4):** The following provides further explanations to the requirements:

4.4.1 Communication Protocol: The nature and extent of the interactions will be influenced both by the objectives of the individuals involved and the context in which the interactions take place. The Professional shall ensure that an effective communication process and protocol is agreed with the Primary Stakeholders and adopted during the engagement. This protocol shall outline various modes and channels of communications, along with the frequency and timelines of communication, also factoring any relevant legal and regulatory provisions. All communications, in whatever form or mode, shall be adequately secured and maintained confidential at all times and shared with other stakeholders with due approvals.

4.4.2 Essential Matters of Communication: Essential matters are those which are necessary for the efficient execution of the engagement. These are agreed between the Professional and the Primary Stakeholder, considering the nature of the engagement and the agreed objectives. Essential Matters are generally in the nature of the following (indicative list):

(a) Written process and protocol of communication, including details of information and cooperation required from Primary and other Stakeholders for access to information sources and for gathering audit evidence.

(b) Scope and methodology of the engagement.

(c) Details of IS laws and regulations applicable to the engagement, including history of any past legal or regulatory infractions.

(d) Reporting format as agreed with the Primary Stakeholders, incorporating any content or format prescribed by legal and regulatory provisions.

4.4.3 Significant Matters of Communication: Significant matters are those which may impact or restrict the scope, methodology, performance or results of the engagement. These matters may be known at the time of finalizing the engagement plan or may surface during the execution phase of the engagement. Significant Matters are generally in the nature of the following (indicative list):

(a) Prevention of access or deliberate withholding of information.

(b) Alteration or destruction of audit evidences.

(c) Lack of support from auditee staff, causing significant delays.

(d) Potential conflict of interest with any Stakeholder.

(e) Restrictions on communication or disclosure in the reports.

(f) Restriction on scope of the audit preventing achievement of objectives.

(g) Any changes or disagreements on Scope, audit observations etc.

(h) Significant deficiencies and weakness in the IS Controls.

(i) Identification of matters concerning frauds or irregularities.

(j) Unacceptable levels of unattended Business or IS risks requiring urgent management attention.

5.0 Documentation of Work Procedures

An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.1 **Engagement Objectives and Planning:**

5.1.1 Minutes of meetings on discussion with Primary stakeholder on the Mandate and engagement objectives.

5.1.2 Engagement Letter detailing the engagement mandate, scope and terms of engagement.

5.1.3 Minutes of meeting with the Business and Information Systems management to establish the context.

5.1.4 Information gathered about the business and its operations, systems and processes and past or known issues.

5.1.5 Copies of Risk Management document reviewed and also prepared to conduct own risk assessment.

5.1.6 Audit Universe and summary of Auditable Units.

5.1.7 Summary of available resources, their competencies and the proper matching of their skills with the audit requirements.

5.1.8 Final overall internal audit plan duly approved by the competent authorities

5.2 **Using the work of an Expert:**

5.2.1 The Professional shall maintain documentation sufficient to demonstrate compliance with this Standard and to support the conclusions drawn from the Expert's work.

5.2.2 An indicative list of Documentation is as follows:

(a) Rationale for engaging the Expert, linked to the complexity or risk of the information system.

(b) Evidence of assessment of the Expert's competence, independence and methodology.

(c) Signed terms of engagement specifying scope, deliverables and confidentiality obligations.

5.2.3 The Professional shall retain the Expert's report and relevant artefacts such as logs, test outputs or configuration extracts that form the basis of audit conclusions.

5.2.4 Where evidence is retained by the auditee or Expert due to legal or proprietary restrictions, a written undertaking shall be obtained confirming safe custody and availability for the prescribed retention period.

5.2.5 All review notes and evaluations relating to the Expert's work shall form part of the audit working papers supporting the final audit opinion.

5.3 **Communication with Stakeholders:**

5.3.1 Communication process and protocol documentation, communication in form of electronic mails and messages, written hardcopy communication.

5.3.2 Documentation to demonstrate compliance with legal and regulatory provisions wherever applicable.

5.3.3 Documentation confirming the communication of Essential and Significant Matters.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 310

ASSIGNMENT EXECUTION

Contents

Paragraph(s)

This Information Systems Audit Standard 310, on "Assignment Execution," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or "Standard") covers the responsibility of the Professional in planning and executing an Information Systems (IS) Audit assignment. It also deals with the work procedures required to conduct the audit assignments with appropriate review and supervision and to execute a work program (also referred to as audit program) in a manner that achieves the engagement objectives and yields reliable, reproducible results.

1.2 Engagement planning at the entity level is covered in ISAS 220 on "Engagement Planning". This Standard, on the other hand, covers the smaller IS audit assignments where some portion of the entity, such as an area, activity or process has been chosen as an auditable unit (refer Para 1.3.3 in ISAS 220).

1.3 **Definitions**: The following terms, along with their definitions, have been used in this Standard.

1.2.1 **Assignment Planning** involves the audit objectives, scope, methodology, and procedures and aligning them with the overall engagement plan or directly with the mandate documented in the engagement letter. The extent of planning will depend, in context and scope, upon the nature, risk and complexity of the IS environment, the size of the entity, and the specific requirements of the stakeholders.

1.2.2 **Work (or audit) program** refers to the structured plan that outlines the specific audit steps or procedures performed to achieve the objectives of the assignment. It serves as the blueprint for executing the audit work.

1.2.3 **Work Procedures** (or Procedures) refer to the specific steps, instructions, and activities undertaken during an IS audit assignment to collect, analyse, and interpret information and data, thereby gathering appropriate and sufficient evidence necessary to support the assignment objectives and conclusions.

1.2.4 **Review** refers to examination of plans, procedures, allocation of resources, evidences collected, the conclusions drawn therefrom, and documentation of work papers, generally undertaken during and post completion of the assignment.

1.2.5 **Supervision** refers to oversight of audit work procedures performed by the audit team members, providing them with overall guidance and their regular monitoring by the Professional.

1.4 **Scope:** This Standard applies to all Information Systems Audit (ISA) assignments, irrespective of the scope and nature of assurance. Where an audit covers only part of an IS environment, the requirements of this Standard shall apply to that extent.

2.0 Objectives

2.1 The objective of this Standard is to ensure that the planning and execution of an ISA assignment is aligned with the engagement objectives and conducted efficiently and effectively in accordance with the agreed scope and stakeholder expectations.

2.2 In achieving the overall objectives, the Professional is guided by the following specific objectives:

(a) Defining the assignment objectives, scope, and approach consistent with engagement mandate and objectives.

(b) That adequate resources, timelines, and technical expertise are identified and appropriately allocated for the effective execution of the assignment.

(c) An approved audit program and well-designed work procedures are executed under appropriate review and supervision.

(d) Progress of the assignment is monitored with the plan and timely remedial action is taken, if required. The plans are updated as and when required and resources are allocated accordingly.

(e) Sufficient, relevant and reliable evidence is obtained through comprehensive process for arriving at conclusion to achieve audit objectives and the same is documented properly.

(f) Work performed is in conformance with the applicable pronouncements of laws, regulations and standards relevant to the audit assignment.

3.0 Requirements

3.1 **<u>Assignment Planning:</u>** The following provides a summary of the key requirements:

3.1.1 The Professional shall understand the engagement level ISA plans, prepared at the entity level, where they exist. In the absence of engagement plans, or where the engagement scope is the same as the scope of assignment, the Professional shall formulate the assignment audit objectives based on the mandate in the engagement letter (refer Para 4.1.1).

3.1.2 The Professional shall establish and document a structured plan for the ISA assignment to ensure systematic coverage of the assignment level scope, and objectives (refer Para 4.1.2)

3.1.3 The planning process shall include the identification of assignment level business dynamics and IS environment context. However, the level of detail in planning shall be commensurate with the nature and complexity of the IS environment limited to the scope of the assignment (refer Para 4.1.3).

3.1.4 The Professional shall hold formal discussions with Stakeholders to confirm assignment objectives, expectations, system boundaries, and constraints affecting scope or timing in order to formulate a comprehensive audit plan (refer Para 4.1.4).

3.1.5 The Professional shall review the management's understanding of the IS risk landscape and undertake an assignment level preliminary IS risk assessment exercise to finalise the scope and objectives (refer Para 4.1.5).

3.1.6 The Professional shall evaluate the required timing and resources (with required competencies) and allocate these based on availability and expertise (refer Para 4.1.6).

3.1.7 The Professional shall, based on all the information gathered, develop an assignment audit strategy and formulate a comprehensive audit plan and documented for due approvals (refer Para 4.1.7).

3.2 **Performing Work Procedures:** The following provides a summary to the key requirements:

3.2.1 The Professional shall execute the assignment work in accordance with the approved Work Program (Audit Program) to cover identified risk and ensure the work is completed within the agreed schedule (refer Para 4.2.1).

3.2.2 The Professional shall obtain and maintain sufficient and appropriate evidence (refer ISAS 320 on "Evidence and Documentation") to support the findings and conclusions drawn, thereby ensuring that the audit objectives are fully achieved (refer para 4.2.2).

3.2.3 The Professional shall apply due scepticism when performing Work Procedures and when evaluating the appropriateness, sufficiency and reliability of the evidence obtained (refer Para 4.2.3).

3.2.4 The Professional shall review and analyse all relevant information, comparing the requirements of the evaluation criteria with the actual conditions in the information system, to identify any differences that may become findings for the assignment (refer Para 4.2.4).

3.2.5 The Professional shall review all identified findings to assess the severity of the associated risk. Where a major risk to the organisation is identified, it shall be formally documented and reported to management for timely and appropriate action (refer Para 4.2.5).

3.3 **Review and Supervision:** The following provides a summary to the key requirements:

3.3.1 The Professional shall use skill sets, knowledge and experience for periodic review and supervision of the assignment based on best professional judgement. The periodicity and extent of review shall be planned after considering all relevant factors but shall ensure that each document is reviewed at least once (refer para 4.3.1).

3.3.2 Review and Supervision by the Professional shall ensure that activities are conducted in line with the planned strategy while adhering to timelines.

3.3.3 The nature of Review and Supervision shall ensure that reliable and sufficient information and evidence is gathered and documented to arrive at a conclusion following standard operating procedures in compliance with statutory requirements.

3.3.4 The Professional shall reassess the nature and extent of review and supervision due to change in circumstances affecting the assignment and make corresponding change and reallocation of resources (refer Para 4.3.2).

3.3.5 Review of work procedures and audit working papers shall be carried out to substantiate audit findings and the evidence of the review and supervision conducted shall be maintained to conform to Standard (refer Para 4.3.3).

4.0 Explanatory Comments

4.1 **Assignment Planning:** The following provides further explanations to the key requirements:

4.1.1 Assignment level planning (refer Para 3.1.1): The planning of an ISA assignment shall be aligned with the overall entity level engagement objectives, which in turn is agreed with the overall engagement mandate received from the primary Stakeholders as covered in ISAS 220 on "Engagement Planning". Assignment level planning will cover a specific auditable unit forming part of the overall engagement plan (such as a specific business location), or a portion of the overall business activity (such as IT application controls) or a specific group of tasks (such as Penetration Testing).

4.1.2 Defining the assignment Scope and Objectives (refer Para 3.1.2): Since the scope of the ISA assignment may be a subset of the scope of the overall IS engagement, the Professional shall build on the entity level understanding, but curtail the scope and objectives to the assignment level only.

4.1.3 Business and IS Context (refer Para 3.1.3): In obtaining an understanding of the business and technology context, the Professional shall have gained requisite understanding of the overall entity level business landscape and IS environment in line with ISAS 210 on "Business and Information Systems

Context". At this stage, the Professional will incorporate this entity level understanding into the assignment level plans and supplement it with greater details at the process level, covering critical applications, specific infrastructure, interfaces, and data flow relevant to the ISA assignment.

4.1.4 Dialogue with Stakeholders (refer para 3.1.4): The Professional shall undertake structured and detailed discussions with all stakeholders (Primary Stakeholders, auditee management, system owners, and other stakeholders) to formulate a comprehensive assignment plan, in line with the similar exercise undertaken at the engagement level as per ISAS 220 on "Engagement Planning". The outcome of these deliberations will help to finalise the audit scope and approach and any constraints affecting the nature of work and timing.

4.1.5 Preliminary IS risk assessment (refer para 3.1.5): The Professional shall use management's assessment of IS risks at the assignment level as a starting point (where available) and conduct a preliminary IS risk assessment covering factors such as reliability and maturity of governance, state of controls and compliance with applicable laws and regulations, ethics and culture.

4.1.6 Timing and resources (refer para 3.1.6): Based on the planned audit procedures, the Professional shall evaluate the time and resources required to conduct an efficient and effective audit. The composition of the audit team is most critical given the need for specialised skills and expertise, and assessing the need to supplement the team with external expertise in line with ISAS 220 covering "Using the work of an Expert". Due consideration shall also be given to planning for appropriate tools, travel and scheduling of various audit activities and communication protocols.

4.1.7 Documented audit plan (refer para 3.1.7): Upon completing all the requisite planning activities, the Professional shall develop a detailed audit strategy, select the appropriate audit approach and methodology for performing the assignment. The plan shall include considerations such as use of technology-enabled audit approaches, automated work programs etc. The assignment plan shall incorporate various factors that impact the nature, timing and extent of audit procedures. The plan shall be reviewed and updated whenever significant changes occur in the technology, operations, or governance framework that could influence the engagement strategy. The documented assignment plan shall be reviewed and approved for implementation as per protocol.

4.2 **Performing Work Procedures:** The following provides further explanations to the requirements:

4.2.1 Assignment Work Program (refer Para 3.2.1): The assignment Work Program details the step-by-step procedures to complete the IS audit. It identifies the criteria used, the specific tasks to achieve the objectives, the methodology (including analytical procedures), and the tools to be deployed. The objectives of the work program include ensuring that the tasks are completed efficiently. If unexpected events, changes in conditions, or audit evidence necessitate modification of planned procedures, the work program shall be adjusted accordingly, and such changes duly approved.

4.2.2 Evidence Collection (refer Para 3.2.2): Evidence shall be sufficient and appropriate. Procedures used to gather the evidence are based on Professional judgement, but may include inquiry and confirmation, observation, inspection, analytical procedures, recalculation/computation, and re-performance. The documentation supporting the evidence shall be appropriate to enable a prudent, informed, and competent person to re-perform the tasks and reach the same conclusion.

4.2.3 Professional Scepticism (refer Para 3.2.3): Exercising professional scepticism requires maintaining an attitude of inquisitiveness and critically assessing the reliability of information. Professional shall apply scepticism when gathering and analysing information to determine if it is relevant, reliable, and sufficient. If information is incomplete, inconsistent, false, or misleading, the Professional shall seek additional evidence.

4.2.4 Analysis of Findings (refer Para 3.2.4): The Professional shall analyse the evidence obtained to determine the actual condition of the information system in relation to the established audit criteria. Where deviations or exceptions are identified, the Professional shall assess their nature, underlying cause, and potential impact on the reliability and security of system processes.

4.2.5 Evaluation of findings (refer Para 3.2.5): The significance of each finding shall be evaluated in terms of its likelihood and severity, and the results prioritised to enable appropriate management response and reporting within the scope of the engagement. If required in the scope of the assignment, the Professional may undertake additional procedures to identify the root cause of the deviations which may eventually allow for corrective actions designed to prevent a repetition of such deviations.

4.3 **Review and Supervision:** The following provides further explanations to the requirements:

4.3.1 Overall Review and Supervision (refer Para 3.3.1): The extent and nature of review and supervision are dependent on various factors such as scope and type of assignment, complexity of technology, laws and regulations, complexity of business operations and competency and expertise of the audit team. The Professional shall apply these factors in assessing the extent and nature of review and supervision to be applied under the circumstances.

4.3.2 Revision of Plan due to change in circumstances (refer Para 3.3.4): The Professional shall reassess the adequacy of review and supervision when the objectives, scope or circumstances change during the course of assignment. In particular rework the time schedule and ensure that requisite skill sets are available with the team and discuss and deliberate with stakeholders.

4.3.3 Review of work procedures (refer Para 3.3.5): The Professional shall evaluate the work procedures to ensure they are in accordance with guidelines provided to team. The evidence gathered is sufficient, reliable and correlate with audit findings. The work procedure ensure that Chain of Custody of evidence (if relevant) is maintained and documented.

5.0 Documentation of Work Procedures

An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.1 **Assignment Planning:**

5.1.1 The methodology and key steps undertaken in the planning process shall be documented to enable confirming their proper execution.

5.1.2 The following documents shall be maintained by the Professional:

(a) Planning methodology or process documentation or checklists, including any technology-enabled tools or templates used in the planning process.

(b) Documentation supporting the information gathered about the business processes, information systems, applications, infrastructure and any past or known system-related issues.

(c) Documentation of any laws and regulations specific to the objectives and scope of the assignment

(d) Documentation of risk assessment process and identification of key risks surrounding the scope as well as performance of the engagement

(e) Summary of meetings and communications with key stakeholders, including management, system owners, and service providers, together with a record of significant inputs or decisions relevant to the audit plan.

(f) Summary of resource requirements, comparison with available competencies, and matching of technical skills such as IT, cybersecurity, or data-analytics expertise with the needs of the assignment.

(g) Copies or references of Information systems architecture, network diagrams, data-flow maps, or control matrices reviewed during planning, (if applicable and part of scope) where such artefacts form the basis of understanding system design and risk exposure.

5.2 **Work Procedures:**

5.2.1 The documentation of work procedures shall be retained as part of the audit working papers and shall contain sufficient and appropriate information and evidence to enable a prudent and competent person to understand the work performed and reach the same conclusions.

5.2.2 The following documents shall be maintained by the Professional:

(a) The approved work program and details of procedures performed, changes approved, and tasks completed.

(b) Evidence that the work performed was consistent with the engagement objectives and scope.

(c) Records of analyses, evaluations, findings, and conclusions, supported by relevant documentary and digital evidence.

(d) Identification of individuals who performed and supervised the work, with evidence of review and approval.

(e) Version control, secure storage, and retention of documents in accordance with defined policies and applicable professional and legal requirements.

5.3 **Review and Supervision:**

5.3.1 Key steps in review and supervision shall be documented and evidenced in writing with signatures of reviewer.

5.3.2 Key findings and evidence obtained shall be documented and chain of custody be preserved.

5.3.3 Minutes of meetings and communication with stakeholders in connection with review and supervision.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1^{st} Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 320

EVIDENCE AND DOCUMENTATION

Contents

Paragraph(s)

This Information Systems Audit Standard 320, on "Evidence and Documentation," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

ISAS EXPOSURE DRAFT
(1st Dec'25)

1.0 Introduction and Scope

1.1 This Information System Audit Standard (ISAS or "Standard") establishes requirements for obtaining, verifying, documenting, and managing Information Systems (IS) audit evidence to support reliable audit conclusions. The Standard also addresses the unique challenges posed by digital artifacts in modern IS audits, where the majority of evidence is electronic and volatile. In addition, it establishes the requirements for preparing, reviewing, storing, and managing the IS audit documentation throughout the audit lifecycle.

1.2 **Definitions**: The following terms, along with their definitions, have been used in this Standard.

1.2.1 **Evidence** refers to data and information collected during an Information Systems Audit to substantiate findings regarding the effectiveness, security, and compliance of IT systems, processes, and controls.

1.2.2 **Direct Evidence** refers to evidence generated by IT systems that directly validates control effectiveness or operational integrity, such as transaction logs, audit trails, system-generated exception reports, or access logs.

1.2.3 **Supporting Evidence** refers to evidence that contextualises or validates IS operations and governance, such as IT policies, change management approvals, incident management records, or Service Level Agreement (SLA) compliance reports.

1.2.4 **Context Specific Evidence** refers to evidence tailored to the organisation's unique IS environment (e.g., On Premises, cloud architectures) along with the legal and regulatory requirements (e.g., IT Act, Companies Act, etc.), ensuring relevance to operational risks and compliance mandates.

1.2.5 **Digital Artifacts** refers to machine or system generated digital objects, such as system logs, configuration logs, meta data, and network traffic data, including screen recordings as well as interactive voice response clips, produced within IT systems.

1.2.6 **Digital Artifacts Lifecycle** denotes the sequential process of identifying, collecting, preserving, analysing digital artifacts and securely purging within an IS audit lifecycle, ensuring each stage maintains their relevance, integrity, and usability as evidence throughout the audit engagement.

1.2.7 **Identification** involves the process of locating and recognising digital artifacts within an IT system, such as detecting system logs recording user activity or configuration files defining server parameters, based on their relevance to the audit's security, performance, or compliance objectives.

1.2.8 **Collection** refers to the systematic gathering of identified digital artifacts using specialised techniques, such as automated log scraping, screen scrapping or secure file extraction, tailored to the artifact's format and the IT environment, ensuring the data remains intact and aligned to audit goals.

1.2.9 **Preservation** describes the secure retention of collected digital artifacts through measures like encryption, access controls, and metadata tagging, protecting their confidentiality, integrity, and availability for the duration of the audit or any subsequent reviews, as well as complying with any statutory retention period requirements.

1.2.10 **Analysis** involves the examination and interpretation of digital artifacts, such as correlating network traffic data with access logs to identify security incidents, using analytical tools to derive findings that support reliable and indisputable audit conclusions.

1.2.11 **Digital Artifact Integrity** refers to the state of a digital artifact being authentic, unaltered, and reflective of its original form as generated by an IT system, verified through techniques such as time stamping, hashing or digital signatures to support its reliability as audit evidence.

1.2.12 **Audit Documentation** refers to the structured record, in electronic or physical form, of audit procedures carried out during an IS audit, the associated evidence captured, and the conclusions derived. This record, forms an essential part of the audit process, capturing the details of IT systems, controls, processes, and support the findings under review.

1.2.13 **Work Papers** refer to the collection of documentation maintained by the Professional that support the audit procedures performed, evidence obtained, and audit findings, and organised systematically to support conclusions reached, facilitate supervision and review, and demonstrate adherence to audit and quality standards.

1.3 **Scope:** This Standard applies to all Information Systems Audit (ISA) assignments, encompassing the evidence and documentation of IT systems, processes, and controls across a wide range of audit assignments, regardless of the nature or complexity of the environment (e.g., cloud architectures, legacy systems) or industry sector. It applies specifically to engagements where digital artifacts are identified, extracted, collected, validated, preserved, analysed and securely destroyed after use as evidence. It encompasses the lifecycle of digital artifacts across diverse IT environments. The Standard is applicable to both internal and external IS audits, including those performed directly by an IS Auditors or with the assistance of IT experts.

2.0 Objectives

2.1 The overall objective of the Standards to ensure that the evidence collected and the documentation prepared by the Professional supports the conclusions reached and forms a reliable basis to form a clear opinion on the results of the ISA assignment.

2.2 The specific objectives of gathering sufficient, appropriate and reliable evidence, including digital artifacts and evidence, are to:

(a) enable the Professional to draw reasonable conclusions that support the scope and objectives of the audit engagement, addressing IS specific risks such as confidentiality, data integrity, and system availability.

(b) provides a structured framework for Professionals to handle digital artifacts, emphasising the use of specialised techniques to maintain their integrity and provide robust audit evidence.

(c) ensure evidence is retained for the time-period specified under statutory and regulatory requirements to facilitate audit review and compliance scrutiny.

2.3 The objectives of preparing complete and sufficient IS audit documentation are to:

(a) validate audit findings and provide the foundation for observations and conclusions drawn from the assessment of IT systems and controls.

(b) assist in the supervision and review of IS audit activities, ensuring consistency across diverse engagements.

(c) demonstrate that the documentation process adheres to established standards and practices applicable to IS audits.

3.0 Requirements

3.1 **<u>Audit Evidence:</u>** The following provides a summary of the key requirements:

3.1.1 The Professional shall obtain sufficient and appropriate audit evidence to form the basis of audit findings and enable reliable conclusions regarding the effectiveness, security, and compliance of IT systems, processes, and controls. Evidence collected through IS audit procedures (e.g., control testing, vulnerability assessments, or log analysis) shall be complementary, relevant to the specific objectives of the IS audit procedure conducted, and aligned with the overall audit scope (refer Para 4.1.1)

3.1.2 The evidence shall be obtained from reliable sources (e.g., system logs, configuration files, access controls, or other IT artifacts) and demonstrate consistency across various evidence types collected. The Professional shall verify the integrity and authenticity of IT related evidence to ensure it accurately reflects the state of the information systems environment (refer Para 4.1.2).

3.1.3 All IS audit evidence collected shall be recorded in a manner that supports traceability and repeatability. The Professional shall maintain a documented process detailing how evidence is gathered, analysed, reviewed, documented, and stored, adhering to quality standards and in conformance with ISAS. Evidence shall be securely stored to protect its confidentiality, integrity, and availability, considering the sensitive nature of IS related data (refer Para 4.1.3).

3.1.4 The Professional shall ensure that audit evidence is collected in alignment with the specific operational context of the organisation's IT environment and complies with applicable regulatory or statutory requirements. This includes tailoring evidence gathering procedures to address industry specific standards, organisational IT policies, and regulations. The Professional shall document how evidence meets these context specific and compliance obligations, ensuring traceability to relevant legal, regulatory, or contractual frameworks (refer Para 4.1.4).

3.2 **Digital Artifacts and Evidence:** The following provides a summary of the key requirements:

3.2.1 The Professional shall obtain and manage digital artifacts as evidence to support audit findings and enable forming conclusions about the security, performance, and compliance of IT systems. These artifacts shall be collected using appropriate techniques directed to specific audit objectives, ensuring they are relevant, complementary, and aligned with the scope of the IS audit engagement (refer Para 4.2.1).

3.2.2 The Professional shall obtain necessary consent from the Auditee, mutually agree on the modalities of requisitioning and exchange digital artifacts and digital evidence. This shall include aspects such as designated electronic channel or computer resource with access to the Professional to be used for exchange of digital artefacts, any restrictions (and solutions) on sharing of digital artifacts or evidence for reasons of confidentiality or such other policy of the Auditee organisation, method of secure transmission or attachments including management of keys and management prescribed retention period, secure purging of such digital artefacts and evidence (refer Para 4.2.2).

3.2.3 Digital artifacts shall be sourced from trustworthy IT systems and verified for integrity and authenticity to reflect the accurate state of the IS environment. The Professional shall ensure consistency across collected artifacts, such as matching timestamps or correlating log entries (refer Para 4.2.2).

3.2.4 All digital artifacts collected during IS audits shall be recorded and stored in a manner that ensures traceability, retrievability and repeatability, with the IS audit function maintaining a documented process for their gathering, identification, inventory, handling, restriction on creating copies thereof, review, preservation, and secure retention. This process must protect the confidentiality, integrity, and availability of these sensitive digital elements, using encryption or access controls to prevent unauthorised alterations or access (refer Para 4.2.3).

3.2.5 The Professional shall ensure all digital artefacts and evidence, including those identified and collected by the Professional are formally routed through the engagement point of contact designated by the Auditee to be sent by recorded communication such as electronic mail or stored in designated computer resource of the Auditee with approved access to the Professional (refer Para 4.2.3).

3.2.6 The Professional shall ensure that the collection and management of digital artifacts are specific to the operational context of the IT environment, complying with applicable regulatory, contractual, or organisational requirements. This includes adjusting collection methods to address the unique characteristics of the IT infrastructure, documenting how these artifacts meet compliance obligations, and maintaining linkages to relevant frameworks to support their legal and audit validity (refer Para 4.2.3).

3.2.7 Where the digital artifacts and evidence are identified, collected etc., by using Automated Tools and Techniques (ATT), this will be done in accordance with ISAS 420 on "Use of Automated Tool and Techniques".

3.3 **Audit Documentation:** The following provides a summary of the key requirements:

3.3.1 The Professional shall document the nature, timing, and extent of completion of all IS audit activities and procedures, including those related to IT systems and controls, in a reproducible format (refer para 4.3.1).

3.3.2 Documentation shall be thorough and adequate to support the analysis of audit findings, the identification of observations, the development of audit reports, and the conclusions drawn from IS audit work. It must clearly indicate the purpose of each procedure, the source of the recorded information, the results of the audit effort, and the identities of the preparer and reviewer (refer Para 4.3.2).

3.3.3 IS audit documentation shall be finalised before the issuance of the final IS audit report, with any remaining administrative tasks completed within a reasonable time-frame following the report's release (refer para 4.3.3).

3.3.4 The IS audit function shall establish a written process outlining the preparation, review, storage, retention and disposal of documentation, ensuring its quality and secure handling to address the sensitivity of IT related data (refer Para 4.3.4).

3.3.5 The ownership and custody of IS audit documentation shall remain with the Professional. When audit tasks are outsourced to an external provider or specialist and the documentation is relied upon for the IS audit report, ownership shall transfer to the Professional. If reliance is placed solely on the third party's report and they retain ownership, arrangements must be made to ensure access to the documentation as needed.

4.0 Explanatory Comments

4.1 **Audit Evidence:** The following provides further explanations to the requirements:

4.1.1 Nature of Evidence (refer Para 3.1.1): Evidence is collected either from the underlying organisation's IT systems, records, configurations, and processes through existing documents supporting IT transactions (e.g., system access logs, configuration files) or IT governance arrangements (e.g., security policies, service level agreements). Alternatively, it is also collected through the performance of IS audit activities and testing procedures by the Professional in one or more of the following methods:

(a) inspection (e.g., reviewing code or hardware)
(b) observation (e.g., monitoring data flows)
(c) recalculation / computation (e.g., analysing performance metrics)
(d) re-performance (e.g., simulating control tests)
(e) analytical review (e.g., anomaly detection in logs)
(f) inquiry (e.g., interviewing IT personnel)
(g) specialised IS audit techniques
(h) using the assistance of IT experts or automated tools.

These sources and procedures, as further categorised in Types of Evidence, include direct evidence and supporting evidence to ensure comprehensive coverage of IT controls.

Sufficiency and appropriateness are inter-related and apply to evidence obtained. Sufficiency refers to the quantity or quantum of evidence gathered, while appropriateness relates to its quality, relevance, and reliability in assessing IT controls, security, and compliance. The types of evidence as described in Para 4.1.4 shall be selected to address risks such as data integrity, cybersecurity threats, or system availability, ensuring that evidence is persuasive on its own and, in aggregate, conclusive in supporting audit findings.

4.1.2 Reliability of Evidence (refer Para 3.1.2) The reliability of IS audit evidence depends on its source (e.g., automated system generated logs vs. manually entered reports), its type (e.g., digital vs. physical), thoroughness (e.g., full vs. sampled data sets), and the timing of the audit procedures conducted (e.g., real time monitoring vs. historical reviews). Reliability may also be enhanced by technical validations like digital signatures, checksums, or audit trails, as applicable to the direct and supporting evidence types.

When the Professional has doubts over the reliability of information collected, such as potential tampering in logs or when evidence from one source (e.g., application logs) is inconsistent with another (e.g., database records), the Professional shall evaluate and modify or expand audit procedures (e.g., by performing forensic analysis or cross-verifying with external sources) to resolve the doubt or conflict, ensuring alignment with the evidence types and context specific IT factors or regulatory requirements.

4.1.3 Evidence Collection Process (refer Para 3.1.3) All IS audit evidence shall be recorded in such a manner that it can be reproduced and reviewed independently of the Professional, including through digital timestamps, hashes for integrity verification, or audit trails. It shall meet certain basic standards of quality to achieve IS audit objectives, including completeness, accuracy, and protection against alteration. The collection and recording process shall encompass the direct and supporting evidence types, such as transaction logs or IT policies, to ensure comprehensive documentation.

Details of these quality standards, the manner in which evidence shall be gathered (e.g., via automated scripts or manual extraction), reviewed for sufficiency and appropriateness, validated for authenticity and reliability (e.g., through hash verification or access logs), and stored (e.g., in encrypted, version-controlled systems), shall be documented in the form of an IS audit process. This process shall also incorporate context specific protocols (e.g., for hybrid IT environments) and regulatory compliance measures (e.g., retention periods under Statutory requirements) to ensure traceability, confidentiality, and defensibility of the evidence types. specified under para 4.1.5.

4.1.4 Context Specific Evidence (refer Para 3.1.4): In line with context specific requirements, evidence collection shall be adapted to the organisation's unique IT environment (e.g., cloud architectures, legacy systems, Internet of Things, Artificial Intelligence), ensuring relevance to operational risks and business objectives. For regulatory or statutory specific requirements, evidence must demonstrate compliance with applicable frameworks (e.g., data protection, information security, payment systems, IT controls over financial reporting). The Professional shall incorporate procedures to gather evidence that directly addresses these mandates, such as privacy impact assessments or compliance logs, and document any deviations or mitigations to support defensible audit conclusions in regulated contexts.

4.1.5 Types of Evidence (refer Para 3.1.1, and 3.1.2): To ensure sufficient and appropriate evidence in an IS audit, the Professional shall collect both Direct Evidence and Supporting Evidence tailored to the organisation's IT environment and regulatory requirements.

Direct Evidence includes data generated by IT systems that directly substantiates control effectiveness or operational integrity, such as transaction logs, audit trails, system-generated exception reports, and access logs or authentication records. These provide verifiable proof of system activities or compliance with controls.

Supporting Evidence includes documentation that contextualises or validates IT operations and governance, such as IT policies and procedures, change management approvals, incident management records, and Service Level Agreement (SLA) compliance reports. These corroborate the operational and compliance framework surrounding direct evidence.

The Professional shall select evidence types that align with the specific IT context (e.g., cloud architectures requiring cloud provider logs, database servers requiring database access logs) and regulatory mandates (e.g., banking requiring encryption logs or Companies Act mandating IT controls over financial reporting, Audit Trails). The Professional shall document the rationale for selecting specific evidence types to ensure relevance, reliability, and traceability to audit objectives.

4.2 Digital Artifacts and Evidence: The following provides further explanations to the requirements:

4.2.1 Nature of Digital Evidence (refer para 3.2.1): Understanding the nature of digital artifacts is key to their effective use in audits, as these elements are shaped by the IT environment in which they reside. Digital artifacts, such as configuration files that dictate system settings or metadata embedded in network traffic, vary depending on whether they originate from cloud platforms, on-premises servers, or legacy systems, each presenting unique characteristics like real-time generation or static storage. The Professional shall recognise how these artifacts reflect the operational context, such as the distributed nature of cloud data or the fixed formats of older systems, allowing them to anticipate challenges like incomplete records or format incompatibilities when planning the audit approach.

4.2.2 Reliability of Digital Evidence (refer para 3.2.2 & 3.2.3): Ensuring the reliability of digital artifacts requires rigorous checks to confirm their trustworthiness as evidence. This involves using tools like hash functions to generate a unique digital fingerprint for system logs, ensuring they haven't been altered, or employing forensic software, if required, to detect tampering in configuration files. Professionals shall verify consistency across artifacts, such as aligning timestamps in network traffic data with access logs, while documenting any limitations, like missing data segments, to maintain an open and dependable audit trail that others can confidently review and rely upon.

4.2.3 Digital Evidence Collection Process (refer para 3.2.3 to 3.2.5): The evidence collection process for digital artifacts involves a structured approach to gather and preserve them effectively. This begins with tailored methods like automated log scraping to collect system logs or secure retrieval of configuration files, ensuring the data is relevant to the audit's focus, such as security controls. Where the Professional has limited access privileges to extract evidence from any system, and has to depend on a system administrator or user to extract digital evidence, the Professional shall perform audit validation and integrity checks on such evidence, before placing reliance on the evidence.

Preservation follows with secure storage in a digital repository, where artifacts are backed up with metadata about their source and collection time, using encryption and access controls to protect against unauthorised changes, allowing the Professional to retrace their steps and maintain a cohesive evidence set. The evidence collection process extends to maintaining and protecting digital artifacts over time to support audit needs. This includes conducting regular integrity checks on stored network traffic data and implementing encrypted backups to safeguard against data loss or breaches, given the sensitive nature of IT information like user activity logs. Professional shall also plan for secure disposal after retention periods, ensuring compliance with privacy standards while keeping the evidence available for future reviews, thus preserving its utility throughout the audit lifecycle.

4.2.4 Types of Digital Evidence: Recognising the types of digital artifacts and evidence helps the Professional identify and utilise the right sources for their audit objectives. These include system logs that record user actions or system events, configuration files that define IT settings, network traffic data that captures communication flows, and metadata that provides context like file creation times. Each type serves a distinct purpose, logs for security audits, configurations for compliance checks, requiring the Professional to select appropriate tools and methods, such as log parsers for logs or packet analysers for traffic data, to extract and analyse them effectively based on the IT environment's needs.

4.3 **Audit Documentation:** The following provides further explanations to the requirements:

4.2.1 Nature of Documentation (refer para 3.2.1): Documentation encompasses a range of records, whether in electronic or physical form, that detail the IS audit procedures performed, the IT related evidence compiled, and the insights gained during the audit process. This may include system logs, configuration details, technical assessments, meeting notes, and correspondence related to significant IT matters, as well as summaries of IT policies or operational data when relevant.

These records may be maintained in either digital or paper-based form, as determined by the Professional, provided they can be reproduced in a verifiable form if required, ensuring their utility across diverse IS audit engagements.

4.2.2 Content of Documentation (refer para 3.2.2): The content and scope of IS audit documentation depend on the judgement of the Professional, as it is neither practical nor essential to record every detail or observation. However, all significant matters involving judgment, particularly those related to IT systems and controls, along with the Professional's conclusions, must be included in the documentation. Effective professional judgment is demonstrated when the documentation supports the objectives above. Additionally, the documentation shall be:

(a) sufficient and comprehensive to eliminate the need for further inquiry;
(b) pertinent and aligned with the goals of the IS audit procedure;
(c) mapped to the requirements and audit scope for demonstration to any regulatory authority;
(d) subject to at least one level of review or approval; and
(e) trustworthy and robust, enabling any quality reviewer to arrive at the same conclusions.

4.2.3 Timely Completion of Documentation (refer para 3.2.3): IS audit work papers shall be assembled into organised files promptly after the conclusion of audit procedures, with any outstanding issues addressed during the preparation of the draft IS audit report. The final IS audit report shall not be issued until all critical IT-related evidence and documentation are fully compiled. The administrative task of finalising the audit files shall be completed within a reasonable time-frame following the release of the final report.

4.2.4 Documentation Process (refer para 3.2.4): IS audit documentation shall be organised and stored systematically as work papers to support the conduct of IS audits, following a defined process that includes quality assurance measures. These measures may involve verifying the completeness of records, ensuring relevance to audit findings and reports, and confirming adherence to established documentation practices.

The documentation shall be retained in line with applicable retention policies and shared only with authorised personnel, with guidance sought from legal advisors or senior management, or the engaging authority for outsourced engagements, before any release to external parties.

5.0 Documentation of Work Procedures

An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.1 Audit Evidence:

5.1.1 Evidence Collection and Sufficiency: Documentation for evidence collection shall include an evidence collection plan that outlines the audit procedures to be performed and their alignment with audit objectives. An evidence inventory shall list all direct evidence and supporting evidence collected, providing a comprehensive record of sources and types. The Professional shall document an evidence sufficiency assessment evaluating the adequacy of quantity and coverage to support audit conclusions, along with an evidence appropriateness evaluation that assesses the relevance and reliability of collected evidence. Work papers shall clearly link evidence collected to specific audit objectives and scope, demonstrating how each piece of evidence contributes to meeting engagement requirements.

5.1.2 Evidence Verification and Reliability: The Professional shall document a source reliability assessment that evaluates the trustworthiness of evidence sources, including system-generated logs, manual records, and third-party reports. Evidence integrity verification records shall include technical validations such as hash values, checksums, or digital signatures that confirm evidence has not been altered. Evidence authenticity validation documentation shall demonstrate procedures performed to confirm that evidence is genuine and originates from claimed sources. A consistency analysis across different evidence types shall be documented to identify and resolve any conflicts or discrepancies. Where reliability doubts or conflicts are identified, resolution documentation shall capture the additional procedures performed, findings, and conclusions reached to address such concerns.

5.1.3 Evidence Recording and Storage: Documentation for evidence recording and storage shall include evidence tracking logs that maintain a complete chain of custody from collection through disposal, recording who accessed evidence, when, and for what purpose. The Professional shall maintain a documented evidence documentation process that details the methods and standards for gathering, reviewing, validating, and storing evidence throughout the audit lifecycle. Evidence storage procedures shall be documented to demonstrate how confidentiality, integrity, and availability of evidence are maintained, including encryption methods, backup procedures, and environmental controls. Access control records for evidence repositories shall document authorisation mechanisms, access logs, and periodic access reviews. Quality standards documentation shall demonstrate that evidence handling meets traceability and repeatability requirements, enabling independent review and verification.

5.1.4 Evidence Verification and Reliability: The Professional shall maintain a regulatory and statutory compliance mapping matrix that links evidence collection activities to applicable legal, regulatory, or contractual requirements. Context-specific evidence collection procedures shall be documented to show how evidence gathering methods are tailored to the organisation's unique IT environment, such as cloud architectures, legacy systems, or hybrid infrastructures. Documentation of alignment with industry-specific standards and organisational policies shall demonstrate how evidence collection conforms to relevant frameworks and internal governance requirements. Traceability documentation shall establish clear linkages between collected evidence and the legal, regulatory, or contractual frameworks they are intended to satisfy. Where deviations from standard procedures are necessary or where mitigating controls are relied upon, deviation or mitigation documentation shall capture the rationale, risk assessment, and compensating measures implemented.

5.1.5 Evidence Collection Techniques Documentation: When employing specific audit procedures, the Professional shall document, the following:

(a) **Inspection:** For inspection procedures, documentation shall include records of IT artifacts examined (such as system logs, configuration files, or codebases), the scope and depth of examination, findings identified, and compliance assessments performed.

(b) **Observation:** Observation procedures shall be documented with details of IT processes observed, timing and duration, individuals present, environmental conditions, and any behavioural changes noted that may affect reliability.

(c) **Recalculation / Computation:** For recalculation and computation procedures, documentation shall capture the calculations performed, tools or methods used (whether manual or computer-assisted audit techniques), input data sources, results obtained, and verification of accuracy against expected outcomes.

(d) **Re-performance:** Re-performance documentation shall detail the control tests simulated, test environment specifications, independence safeguards implemented, results obtained, and validation of design and operating effectiveness.

(e) **Analytical Procedures:** Analytical procedures documentation shall include descriptions of data analysed, analytical tools or techniques employed (such as computer-assisted audit techniques or SIEM systems), relationships or patterns identified, trends observed, anomalies detected, and conclusions drawn.

(f) **Inquiry:** Inquiry procedures shall be documented with records of inquiries made (whether formal or informal), identification of individuals contacted and their roles, questions asked, responses received, and any corroborating documentation obtained.

(g) **Specialised IS Audit Techniques:** For specialised IS audit techniques such as vulnerability scanning, penetration testing, or forensic analysis, documentation shall capture the techniques employed, scope and objectives, tools and methodologies used, findings and risk ratings, and confirmation of compliance with ICAI standards and ethical guidelines.

5.2 Digital Evidence:

5.2.1 **Description:** The Professional shall document the scope of each procedure, detailing the specific digital artifacts targeted (e.g., access logs, metadata) and provide a description of the approach, including the tools and techniques applied, to reflect the audit's objectives and the IT environment's complexity.

5.2.2 **Tools and Techniques Applied:** The Professional shall record the specific tools and techniques used, such as log parsers, forensic software, if applied, or hash verification methods, specifying their application to extract /collect, validate, and analyse digital artifacts, and noting any limitations or adjustments made to accommodate diverse IT systems like cloud platforms or legacy databases.

5.2.3 **Outcomes and Findings:** The Professional shall document the outcomes of each procedure, including any findings, anomalies, or conclusions derived from analysing digital artifacts, linking them to the evidence collected (e.g., correlating network traffic data with security incidents) to provide a clear basis for audit observations and reports.

5.2.4 **Review and Validation:** The Professional shall ensure that the documented procedures undergo at least one level of review to verify accuracy, completeness, and alignment with the Standards, maintaining a record of the review process, including feedback or corrections, to demonstrate conformance and facilitate peer evaluation.

5.2.5 **Pre-Report Completion:** The Professional shall assemble digital artifact work papers into organised files promptly after completing audit procedures, addressing any outstanding issues during the draft reporting stage, and ensure the final IS audit report is not released until all significant digital evidence is fully documented and validated.

5.2.6 **Post-Report Administration:** The administrative process of finalising digital artifact files, including organisation, secure storage, and retention planning, shall be completed within a reasonable time-frame of the release of the final, ensuring all documentation is ready for review, retention, or disposal in accordance with security and compliance requirements.

5.3 **Audit Documentation:** The nature of evidence and documentation expected to demonstrate conformance to the Standards shall be achieved by the Professional thoroughly documenting the procedures employed during IS audit activities. This documentation shall capture the methods used to assess IT systems, monitor operational controls, validate system outputs, test IT processes, analyse data, gather information, and apply specialised techniques, ensuring a robust and traceable record to support audit objectives and compliance.

5.3.1 **<u>Description</u>**

The Professional shall document the scope of each procedure, including the specific IT components or controls targeted (e.g., network configurations, access logs), and provide a detailed description of the approach, ensuring it reflects the audit's objectives and the IT environment's complexity.

5.3.2 **<u>Tools and Techniques</u>**

The Professional shall record the tools, techniques, or automated methods (e.g., computer-assisted audit techniques, vulnerability scanners) utilised during the procedures, specifying their application and any limitations, to ensure the documentation supports the reliability and reproducibility of the audit work.

5.3.3 **Outcomes and Findings**

The Professional shall document the outcomes of each procedure, including any findings, anomalies, or conclusions related to IT systems and controls, linking them to the evidence collected to provide a clear basis for audit observations and reports.

5.3.4 **Review and Validation**

The Professional shall ensure that the documented procedures undergo at least one level of review to verify accuracy, completeness, and alignment with the Standards, maintaining a record of the review process to demonstrate conformance and facilitate peer evaluation.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 410

AUDIT OF INFORMATION SYSTEMS CONTROLS

Contents

Paragraph(s)

This Information Systems Audit Standard 410, on "Audit of Information Systems Controls," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or “Standard”) specifies requirements for performing audits of Information Systems (IS) Controls, which covers both Information Technology General Controls (ITGC) that operate at the entity level and Application Controls, that are embedded in the supporting application software.

1.2 ITGC are pervasive controls that apply across the whole IT environment (compute, storage and network) and provide the foundation for reliable processing of transactions, maintenance of data integrity, and operation of application controls. These controls are in the nature of IT Governance Controls, and across the whole technology environment, such as Access Controls, Security Management controls, and Technical Configuration Controls, etc.

1.3 Application controls are integral to ensuring the accuracy, completeness, validity, authorization, and integrity of business transactions and data processed through business and supporting applications. Business applications may be deployed across diverse technology environments using heterogenous technologies. The requirements specified herein apply regardless of the underlying technology architecture.

1.4 **Definitions**: The following terms, along with their definitions, have been used in this Standard:

1.4.1 **IT General Controls (ITGC)** are pervasive entity level controls such as IT governance controls or that apply across the information technology environment (compute, storage and network) and provide the foundation for reliable processing of transactions, maintenance of data integrity, and operation of application controls.

1.4.2 **ITGC Audit** is the audit of design and operating effectiveness of the ITGC.

1.4.3 **Service Organization:** A third-party entity that provides one or more business process automation services, or information systems or technology services, that are relevant to the Internal Controls over Financial Reporting (ICFR) or internal controls relevant to the business and supporting processes.

1.4.4 **Complementary User Entity Controls (CUECs):** Controls that a user organisation must implement and operate to complement service organisation controls for the overall control framework to be effective.

1.4.5 **Application Controls** are internal controls embedded within business applications operating at the transaction or data processing level, designed to ensure completeness, accuracy, validity, authorisation, compliance and integrity of business transactions and data throughout input, processing, storage, and output phases.

Application controls are broadly of two types:

(a) Functional Controls which are embedded within the business and operational logic that the applications automate, and

(b) Security Controls that mitigate the inherent IT security risks relevant to the application.

1.4.6 **Automated Controls:** Controls performed by an application system with minimal or no manual intervention, operating through programmed logic, validation rules, and/or system configurations.

1.4.7 **IT-Dependent Controls:** Manual controls whose effectiveness depends on the completeness and accuracy of information produced by application systems.

1.4.8 **Application Security Controls** mitigate the inherent risks to confidentiality, integrity, availability and privacy arising from use of technology for automation of business processes and associated transaction and data processing.

1.5 **Scope:** This Standard is applicable to the design and/or operating effectiveness of the IS Controls (regardless of size, nature and complexity of underlying technology architecture and IT eco-system), either:

(a) Independent audit of IS Controls as a standalone engagement; or

(b) Audit of IS Controls as an integral component of any other IS audit engagement where reliance on IS Controls is necessary to support audit conclusions.

2.0 Objectives

2.1 The primary objective of this Standard is to enable the Professional to conclude whether IS Controls (i.e., ITGC and Application Controls) are suitably designed, implemented and operating effectively to meet specific control objectives.

2.2 The Specific objectives supporting this overall objective are as follows:

(a) To identify the scope of IS Controls and its components relevant to the engagement objectives and scope.

(b) To establish requirements for planning and performing an audit of IS controls, that ensure the completeness, accuracy, validity, authorization, integrity, confidentiality, availability, timeliness and reliability of the IS general environment and prevalent applications.

(c) To undertake an IS risk assessment considering inherent technology risks and control design vulnerabilities and the materiality and significance of IS to business processes, while appreciating the pervasiveness of IT across multiple applications and systems.

(d) To ensure consistent and reliable audit execution and reporting by emphasizing the use of automated tools and techniques (ATTs), validation of system-generated information, and comprehensive documentation of planning, testing, evaluation, and conclusions supporting the assurance provided.

3.0 Requirements

3.1 **Audit of IT General Controls:** The following provides a summary of the key requirements:

3.1.1 The Professional shall obtain an understanding of the Information Systems (IS) environment and the IS eco-system in which the entity operates, with a view to identify the IT universe and key ITGC components relevant to the engagement scope and objectives (refer Para 4.1.1 and Para 4.1.2).

3.1.2 The Professional shall perform risk assessment to identify key technology risks including unauthorised system or data changes, inappropriate access, system failures, data loss or corruption, IT regulatory and contractual risks, third-party service provider risks, and system unavailability due to disasters or major disruptions. These procedures shall be undertaken as per ISAS 110 covering "Information Systems Risk Management" (refer Para 4.1.2).

3.1.3 The Professional shall, based on such risk assessment, confirm or propose modifications to the audit objectives and scope specifying in-scope IT systems, relevant ITGC components to be included in-scope, including any systems interfaces with external systems, third party service providers (refer Para 4.1.3).

3.1.4 The Professional shall confirm and document the engagement mandate, scope and coverage of ITGC components, intended users, subject matter, criteria, reporting form, and period of examination (refer Para 4.1.3).

3.1.5 The Professional shall formulate appropriate audit testing procedures to evaluate whether controls are suitably designed and implemented across the relevant IT layers (refer Para 4.1.4).

3.1.6 The Professional shall perform operating effectiveness testing to obtain evidence that controls operate as designed throughout the audit period. For automated IT controls that are subject to robust governance and change management controls test-of-one approach may be adopted. For manual controls, the Professional shall draw appropriate samples to be selected using statistical or judgmental methods. The nature, timing, and extent of testing shall be determined based on assessed risk, control nature, frequency, pervasiveness, and reliance to be placed (refer Para 4.1.5 to 4.1.7).

3.1.7 Where ITGCs operate in conjunction with application controls or business process controls, the Professional shall consider the complementary nature of controls and test the integrated control environment, depending on the scope of the engagement. Where ITGCs are operated by third-party service providers, hosting providers, managed service providers, or through shared service arrangements, the Professional shall consider applicable Service Organization Control Reports (SOCR) and evaluate complementary user entity controls where relevant (refer Para 4.1.8).

3.1.8 The Professional shall consider use of specialized IT audit tools and Automated Tools and Techniques (ATT) where they provide efficient or effective audit means, and shall understand tool functionality, limitations, and verify accuracy and completeness of extracted data (refer Para 4.1.9).

3.1.9 The Professional shall, after co-relation of findings and drawing conclusions on any control deficiencies, formally communicate to management and IT leadership on timely basis. (refer Para 4.1.10).

3.2 **Audit of Application Controls:** The following provides a summary of the key requirements:

3.2.1 The Professional shall obtain requisite understanding of the application environment, associated business context and business processes, entity level controls, extent of automation and in context use such information in confirming or to propose modification of the engagement objectives, applications in scope, subject matter, criteria, and period of examination (refer para 4.2.1).

3.2.2 In planning the engagement, the Professional shall identify any risks to the completeness, accuracy, validity, authorization, integrity, compliance, confidentiality, availability and timeliness of transactions and data processed through the applications in scope and associated dependencies on other applications. The Professional shall also consider any significant outcomes of such risk assessment that may have require modification or refinement of the scope of the engagement and the audit program (refer para 4.2.2).

3.2.3 The Professional shall, in consideration of the scope of the engagement, accordingly plan and perform the audit of design and operating effectiveness of automated and IT-dependent controls that cover the completeness, accuracy, validity, authorization, integrity, compliance, confidentiality, availability and timeliness of transactions and data processed through the applications in scope (refer para 4.2.2).

3.2.4 Unless otherwise limited or specified by the objective and the scope of the engagement, a comprehensive application audit shall include an audit of the design and operating effectiveness of the Functional controls (business internal controls embedded within the application), am audit of associated IT general and governance controls, and an audit of the Security controls (including security of integration and interface controls) in addition to the automated controls. (refer para 4.2.3 and 4.2.4).

3.2.5 The Professional shall assess the dependency of automated application controls on the underlying IT general and governance controls. Based on the results of such testing, the Professional shall consider the extent of reliance that can be placed on the application controls and accordingly modify the audit procedures (refer para 4.2.5).

3.2.6 The Professional shall consider using Automated Tools and Techniques (ATT) where they provide efficient or effective means of automating audit procedures subject to prior risk assessment of using proposed tools, comprehensive audit of such tools to satisfy the accuracy, consistency, reliability, security and compliance. Where feasible, the Professional shall consider testing the complete population of critical transactions automated within an application, as against samples using ATTs (refer para 4.2.6).

3.2.7 Where application controls are operated by third-party service providers or through shared service arrangements, the Professional shall consider placing reliance on applicable service organization control reports and evaluate complementary user entity controls to the extent these are relevant to the scope of the engagement (refer para 4.2.7)

4.0 Explanatory Comments

4.1 **Auditing IT General Controls:** The following provides further explanations to the key requirements:

4.1.1 Understanding the IS environment and ITGC ecosystem (refer Para 3.1.1): An ITGC audit requires a comprehensive understanding of the business process landscape and the whole IS environment and the ITGC ecosystem within that landscape, such as IT governance and organisational structures, in-scope systems and infrastructure, IT service providers, technology architecture, IT policies and procedures, and technical architecture, IT components and IT technology controls. These procedures shall be undertaken in line with ISAS 210 on "Business and Information Systems Context".

4.1.2 IT General and Governance Controls (refer Para 3.1.1): These controls govern the organisation's direction and oversight of IT functions such as IT governance structures, policy framework, roles and responsibilities including segregation of duties, IT risk management, change management, identity and access management, systems development life cycle controls, third party management, IT regulatory compliance, and emerging technologies such as artificial intelligence.

(a) IT Technology Controls: These are the technical controls implemented within IT infrastructure, platforms, and systems such as database management controls, network security, security management server and end point security, detective controls and monitoring, configuration management, cryptographic controls, backup and resilience controls, physical and environmental controls, cloud service provider controls.

(b) IT General and Governance Controls: These are the controls that establish organizational framework, policies, processes, and accountability structures governing IT operations, including IT governance and oversight, IT policies and procedures, IT organisational structure and segregation of duties, change management, access administration, program development and system acquisition, vendor and third-party management, and disaster recovery and business continuity.

4.1.3 Scoping of the ITGC audit (refer Para 3.1.3 and 3.1.4): ITGC scope should be determined based on, where applicable, in-scope applications and their underlying technology infrastructure and its components, exclusion of ITGC for out-of-scope systems, consideration of shared infrastructure, and identification of service provider versus user organisation responsibilities for cloud or SaaS applications. The criteria for confirming scope may include factors such as:

(a) In-scope IT systems and infrastructure components.

(b) IT processes and organisational structures.

(c) Critical IT service providers and vendor relationships.

(d) Relevant IT policies, standards, and procedures.

(e) Key IT personnel and segregation of duties requirements.

4.1.4 Formulation of Testing Procedures (refer Para 3.1.5): Design and implementation testing includes review of IT policies and procedures, interviews with IT personnel, observation of activities, inspection of system configurations, walkthroughs, and review of organizational charts. Operating effectiveness testing procedures includes sampling for manual controls, configuration testing for automated controls, testing for cybersecurity controls using automated tools, inspection of management review evidence, and extraction of system-generated logs and audit trails.

4.1.5 Executing Testing Procedures (refer Para 3.1.6): The Professional shall identify the linkages between any applications or business processes in scope of the larger engagement scope such as those relevant to the Internal Controls over Financial Reporting (ICFR) and underlying ITGC components relevant to the accurate, consistent and reliable operation of such applications. The Professional shall appropriately incorporate such ITGC components including the controls across Information Technology layers (database, middleware, operating systems, firmware, infrastructure components) to be tested in the work program including the nature and extent of testing (including Test-of-one) to be performed, co-relation of results, identification of weaknesses and residual risks, as are necessary to meet the respective control objectives.

4.1.6 Nature of Testing for Automated IT Controls (refer Para 3.1.6): For automated IT controls that are subject to robust governance and change management controls test-of-one approach may be adopted. Professional may test control configuration at point in time and verify configuration remained unchanged during audit period through review of change logs, confirmation with IT personnel, and period-end testing. Test-of-one is only appropriate when higher-level change management controls are effective.

4.1.7 Nature of Testing for Manual IT Controls (refer Para 3.1.6): For manual controls, the Professional shall draw appropriate samples to be selected using statistical or judgmental methods. The nature, timing, and extent of testing shall be determined based on assessed risk, control nature, frequency, pervasiveness, and reliance to be placed.

4.1.8 Service Provider Environments (refer Para 3.1.7): When IT functions are performed by service providers, Professional shall understand shared responsibility model, obtain and evaluate Service Organization Control Reports (SOC 1, SOC 2, ISAE 3402), identify and test Complementary User Entity Controls (CUECs), assess carve-outs and exceptions in service provider reports, and address bridge periods where service provider reports do not cover full audit period.

4.1.9 Sampling Considerations: Sample sizes shall be determined based on control frequency (daily controls require larger samples; periodic controls may test all instances), population size, risk and materiality levels, prior period results, and nature of testing (system-generated evidence may allow complete population analysis; manual evidence requires sampling). Professional shall document sampling methodology and rationale.

4.1.10 Reporting of Control Deficiencies (refer Para 3.1.9): Where the Professional comes across any significant deficiencies and material weaknesses, these shall be clearly identified separately and formally communicated to those charged with governance. Where the ITGC audit supports the reliable operation of business and supporting applications, the Professional shall communicate the impact of ITGC deficiencies on application control reliability and overall audit conclusions.

4.2 **Auditing Application Controls:** The following provides further explanations to the key requirements:

4.2.1 Understanding the application environment (refer Para 3.2.1): An application audit requires comprehensive understanding of the business process landscape, application architecture, data flows, configurable parameters, user roles, and integration touchpoints. The Professional should obtain this understanding through walkthroughs, system documentation review, and discussions with key stakeholders. Such understanding enables accurate identification of applications in scope, relevant modules, associated entity-level controls, and interdependencies on other systems for transaction processing, thereby informing engagement objectives, subject matter, and criteria.

4.2.2 Automated controls (refer Para 3.2.3): These operate through programmed logic and can often be tested through a "test-of-one" approach if IT general controls are effective and the control logic has not changed during the period. For IT-dependent manual controls, the Professional shall validate the completeness, accuracy, and definition of system-generated information (IPE) before relying upon it. This ensures that audit evidence derived from system outputs is reliable and consistent with management's assertions.

4.2.3 Application functional controls (refer Para 3.2.4): are embedded within application logic to ensure data integrity and proper transaction processing. These include input controls (validity, completeness, accuracy), processing controls (correct computation per business rules), output controls (proper distribution and reporting), master data controls (reference data integrity), configurable parameters (appropriate and authorized settings), and interface controls (complete and accurate data transfer). The Professional should identify and assess these control types to ensure completeness of audit coverage.

4.2.4 Application security controls (refer Para 3.2.4): govern user access and data protection at the application layer. These include authentication, authorisation, role-based access, segregation of duties, configuration protection, audit trails, and data protection mechanisms. The Professional should assess both preventive and detective controls, as well as compensating mechanisms where segregation of duties conflicts exist, such as exception reviews or enhanced monitoring. Dependencies on IT general and governance controls, such as change management and logical access controls, must be carefully evaluated to determine the reliability of application controls.

4.2.5 Configurable parameter settings: Where applications rely on configurable parameters or business rules, the Professional should evaluate both the appropriateness and authorisation of parameter settings, as well as their operational effectiveness. Parameter changes during the audit period must be traced to confirm authorised and controlled modifications. Interface and integration controls should also be examined for completeness, accuracy, validity, and error handling across system boundaries, including reconciliation of records between source and target systems.

4.2.6 Deployment of Automated Tools and Techniques (refer Para 3.2.6): Where feasible, the Professional shall employ Automated Tools and Techniques (ATTs) to enhance efficiency and assurance coverage, including data analytics, exception identification, or full-population testing of automated transactions. Before deployment, the Professional must evaluate such tools for accuracy, reliability, consistency, and security. Use of ATT should be risk-assessed, and evidence obtained should be properly retained to support audit conclusions.

4.2.7 Third-party Service providers (refer Para 3.2.7): Where the in-scope application is hosted or managed by a service provider, the Professional should obtain assurance reports (e.g., Service Organisation Control Report, SOC 1/SOC 2) and evaluate complementary user entity controls to ensure that the control environment relevant to application processing remains effective. Identified exceptions or carve-outs in service provider reports should be considered in determining audit risk and the sufficiency of procedures performed at the user entity.

4.2.8 Evaluation and Reporting of Control Deficiencies: Control deficiencies identified during the engagement shall be evaluated based on likelihood and magnitude of potential misstatement or operational impact. Deficiencies may be classified as control deficiency, significant deficiency, or material weakness. The Professional shall exercise judgment in considering compensating controls and the pervasiveness of the issue.

Engagement reporting shall clearly describe the subject matter, criteria, scope, approach, findings, conclusions, and management responses.

5.0 Documentation of Work Procedures

An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.1 **Documentation for audit of ITGC:**

5.1.1 An understanding of IT environment, IT risk assessment, scoping decisions, audit program, and linkage of ITGC to in-scope applications.

5.1.2 ITGC control matrices mapping controls to objectives, IT policies and procedures reviewed, organisational structure and segregation of duties analysis, design and implementation test evidence, operating effectiveness test evidence, system configurations, and audit logs analysed depending upon the scope in place.

5.1.3 Service provider control reports obtained, evaluation of service auditor opinions, CUEC identification and testing, and bridge period analysis.

5.1.4 Automated Tools and Techniques (ATT) documentation including tools used, queries executed, and results analysis.

5.1.5 Exception analysis, ITGC deficiency classification, pervasiveness assessment, impact on application control reliability, compensating controls evaluation, and impact on audit conclusions.

5.2 **Documentation for audit of Application Controls:**

5.2.1 An understanding obtained of the application environment and related business processes.

5.2.2 The identification of control objectives, risks, and corresponding application controls;

5.2.3 The design and execution of audit procedures (manual and automated); and the basis for conclusions on design and operating effectiveness.

5.2.4 An illustrative list of documentation of work performed is as follows:

(a) Application architecture, modules, data flows, configurable parameters, and process walkthroughs linking business functions with system logic and key integration touchpoints.

(b) Matrix linking application risks to functional, security, and interface controls with related assertions, control objectives, and dependencies on IT general controls.

(c) Tests for design and operating effectiveness, sampling rationale, use of ATTs, population details, and justification for test-of-one or manual sampling.

(d) Walkthrough notes, configuration screenshots, parameter listings, and inspection evidence confirming correct design, implementation, and authorization of application control settings.

(e) Test execution results, IPE validation, audit trail reviews, system logs, ATT outputs, and exceptions identified during control operation testing.

(f) Reliance on ITGCs, exceptions identified, compensating controls and implications for completeness, accuracy, or validity of automated control operations

(g) Control test results, classification of deficiencies, management responses, auditor conclusions, and review sign-offs linking findings to control objectives and assertions.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 420

USE OF AUTOMATED TOOLS AND TECHNIQUES

Contents

Paragraph(s)

This Information Systems Audit Standard 420, on "Use of Automated Tools and Techniques," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or "Standard") specifies requirements where a Professional uses any Automated Tools and Techniques (ATT), emerging technologies such as artificial intelligence (AI), Internet of Things (IoT), Blockchain, Big Data, Advanced data analytics when conducting Information Systems (IS) audit engagements.

1.2 Use of ATT in audit engagements enhances audit quality by enabling comprehensive data analysis, automation of audit procedures, identification of anomalies, and deeper evaluation of control effectiveness. In context of the significant and complex digital transformation of enterprises, the use of such automated tools, technology and techniques is indispensable to perform audit procedures especially cybersecurity test procedures.

1.3 This Standard recognizes that while technology enhances audit capabilities, it also introduces risks to accuracy, data integrity, data leak, consistency, reliability and confidentiality of data accessed by such tools. Risks arising from deployment of such tools and technology in an Organisation's IS environment could lead to incorrect conclusions and audit assurance.

1.4 **Definitions**: The following terms, along with their definitions, have been used in this Standard:

1.4.1 **Automated Tools and Techniques (ATT):** Automated tools such as software, applications, platforms, algorithms, emerging technologies, and automated techniques, used in engagement planning, automated audit procedures including extracting, analysing, testing data from information systems, identifying and scoring findings and reporting thereon.

1.4.2 **Reproducibility of Results:** Reproducibility refers to the ability of any audit tool, technique, or AI model to produce identical or consistent results when applied repeatedly to the same dataset under the same conditions and parameters. Reproducibility is a fundamental requirement for tool reliability and enables verification of tool accuracy and detection of tool defects or environmental issues. The consistency of results by using ATT is critical.

1.5 **Scope:** This Standard is applicable to engagements where the Professional uses ATT in partial or significant automation of audit procedures and further extending to other phases of the engagement such as engagement planning, risk assessment, engagement management, automation of audit procedures, analysis of artifacts and evidence and report preparation. The Standard is also applicable to such technologies used by experts engaged by the Professional or where the Professional uses third party software, platforms or tools.

2.0 Objectives

2.1 The primary objective of this Standard is to guide the Professional when using ATTs in IS audit engagements to enhance the overall quality and efficiency of the audit and its outcome.

2.2 The Standard addresses this through the following specific objectives:

(a) The ATT to be deployed is selected in a methodical and consistent manner by evaluating the available tools, supported by robust quality control measures and through a continuous competence development program.

(b) The use of ATT and AI is reliable, secure, transparent, and subject to proper validation, ethical safeguards and through informed professional expertise.

(c) The deployment of ATT is properly planned, supervised, and executed with competence and due care, produces reliable and valid results, safeguards data security and confidentiality, is appropriately documented to support audit conclusions, and complies with all applicable professional standards.

3.0 Requirements

3.1 The Professional shall evaluate the appropriateness, scope, and extent of technology and tools to be used in the IS audit engagement based on the understanding of the business and IS environment context and the nature, complexity, and objectives of the engagement (refer Para 4.1).

3.2 The Professional shall establish governance controls for the selection, risk assessment, approval, validation, reproducibility, accreditation, versioning, change management, and oversight of technology and tools, including those incorporating special considerations for use of emerging technologies such as artificial intelligence (refer Para 4.2).

3.3 The Professional shall identify, assess, and respond to risks arising from the use of technology and tools, including risks related to reliability, consistent performance, data integrity, cybersecurity, legal or regulatory compliance, and competency (refer Para 4.3).

3.4 The Professional shall evaluate the availability, accessibility, reliability, and suitability of data within the prevailing IS and determine related resource requirements, including competent personnel, infrastructure, and deployment considerations. The Professional shall also consider legal, regulatory, and cross-border data obligations (refer Para 4.4).

3.5 The Professional shall possess, or obtain, adequate competence to use the selected technology and tools. Where such competence is insufficient, the Professional shall engage specialists with appropriate expertise (refer Para 4.5).

3.6 The Professional shall exercise due care when approving and onboarding technology and tools based on an accreditation by determining their functionality, integrity, accuracy, security, and potential impact on the IS. The Professional shall communicate to the relevant stakeholders the technology and tools to be used, the nature of automated procedures, the associated risks, and (if required) obtain appropriate authorisation before use (refer para 4.6).

3.7 The Professional shall maintain professional scepticism when using outputs from automated tools, including requisite attention to those using artificial intelligence, and shall obtain sufficient and appropriate evidence to support conclusions. The Professional shall ensure that processing and retention of sensitive or regulated data comply with confidentiality, privacy, and data protection requirements (refer Para 4.7).

4.0 Explanatory Comments

4.1 **Selection of Tools and Technology (refer Para 3.1):** The criteria to apply when selecting which ATT to deploy would include, automated data extraction and analytics, publicly available or custom audit tools, GenAI chatbots, machine-learning and NLP models, Robotic Process Automation for audit process automation, continuous-monitoring utilities, and log co-relation and analysis, security testing tools and the like, that enhance audit capability when aligned with audit objectives and professional judgment.

4.2 **Establish governance controls (refer Para 3.2):** Use of tools and technology in auditing bears significant benefits as well as risks, hence a structured governance framework ensures all key aspects are considered and dealt with in a structured and systematic manner with clear roles, responsibilities, oversight and reporting requirements. These may include aspects such as process or methodology for communication and obtaining approval, accreditation criteria for tool on boarding, validation and reproducibility of tool performance, version control, change management, and authorization processes protect engagements from inappropriate deployment or irresponsible use, including when using emerging technologies such as AI-enabled GenAI tools and third-party technologies in the auditee's environment.

4.3 **Risk of ATT (refer Para 3.3):** ATT and AI introduce risks such as opacity, embedded bias, non-deterministic outcomes, and misinterpretation of correlations as conclusions. Understanding how these tools and models operate, their training data, and their inherent limitations supports ethical, transparent, and controlled use within audit engagements.

4.4 **ATT evaluation (refer Para 3.4):** Data characteristics significantly influence the reliability of technology-enabled procedures. Understanding data lineage, completeness, transformations, system constraints, and regulatory conditions enables the Professional to judge whether technology-driven analyses produce valid audit evidence and whether data handling meets privacy and legal expectations.

4.5 **Competence (refer Para 3.5)**: The competence in technology enables the Professional to appropriately challenge outputs, detect anomalies, and recognise results which are inconsistent with expectations. Relying on specialists does not diminish the Professional's responsibility to understand key implications of technology-enabled work and exercise informed judgment.

4.6 **Reliability (refer Para 3.6):** Automated outputs may appear precise yet be misleading without corroboration. Reproducibility testing and sensitivity analysis provide assurance that tools behave consistently. Unexpected variations signal model instability, configuration issues, or flawed datasets, requiring deeper investigation before reliance.

4.7 **Comprehensive documentation (refer Para 3.7):** Audit documentation strengthens audit defensibility, facilitates internal review and regulatory scrutiny, and supports reproducibility of results. Recording decisions, parameters, validations, and interpretations ensures transparency, allows independent reperformance, and demonstrates that professional judgment, not automation underpins audit conclusions.

5.0 Documentation of Work Procedures

5.1 The Professional shall document considerations taken into account when selecting specific ATT to deploy, such as an assessment of the information systems environment, scope and extent of technology-enabled procedures, expected outcomes, limitations considered, risks evaluated, and justification for choosing automated over manual techniques.

5.2 An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.2.1 Governance documentation may include evidence of tool approval or accreditation, version-control and change-management records, AI guardrail approvals, vendor due-diligence summaries, alignment with firm governance policies, authorization for use in the auditee environment, and records of validation or initial testing.

5.2.2 Risk-related documentation may include assessments of tool reliability and performance risks, data integrity and cybersecurity considerations, legal and regulatory exposures, competence risks, mitigation measures applied, monitoring of tool results, and evaluation of residual risks affecting audit conclusions.

5.2.3 Data-related documentation may include assessments of data availability and access, data lineage and reliability considerations, resource and competency needs, infrastructure constraints, legal and cross-border data implications, auditee confirmations, and identified data-quality limitations or restrictions.

5.2.4 Competence documentation may reflect evaluations of required skills, training undertaken, involvement and assessment of specialists, defined scope of specialist work, review procedures performed by the Professional, independence considerations, and identified competence gaps with planned mitigation actions.

5.2.5 Due care documentation may include tool validation outcomes, benchmark testing, communications to the auditee on intended technology use, auditee authorization for automated procedures, assessments of security and system impact, vendor reliability evaluations, and approvals for AI or external platforms.

5.2.6 Professional judgment documentation may include corroboration procedures for automated outputs, evaluation of anomalies highlighted by tools, records of human oversight over AI-generated results, noted limitations in tool outputs, scepticism applied to exceptions, privacy compliance, and manual verification steps performed.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1^{st} Dec’25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 430

AUDIT OF DIGITAL PERSONAL DATA PROTECTION

Contents

This Information Systems Audit Standard 430, on “Audit of Digital Personal Data Protection,” issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the “Preface to the Information Systems Audit Standards”, the “Framework Governing Information Systems Audit Standards” and “Basic Principles of Information Systems Audit” issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or "Standard") 450 deals with specific types of IS audit engagement related to Digital Personal Data Protection.

1.2 The Subject Matter of these engagements generally requires evaluation of procedures, internal control structures adopted and compliances to legal or regulatory requirements.

1.3 **Definitions**: The following terms, along with their definitions, have been used in this Standard:

1.3.1 **Digital Personal Data (DPD):** Data of a personal nature of an Individual in digital form by which the individual is identifiable.

1.3.2 **Protection of DPD:** The Digital Personal Data is protected from unauthorised or accidental disclosure or sharing, inappropriate use, unauthorised modification, loss of access, destruction or by any other way the integrity, availability or confidentiality of which is compromised.

1.4 **Scope:**

The standard is applicable to all IS audit engagements related to Protection of Digital Personal Data as a subject matter.

2.0 Objectives

2.1 The Objective of a Standard on Audit of Digital Personal Data Protection is to outline the responsibilities of a Professional conducting an IS audit engagement as per prevailing Data Protection laws and regulations, as applicable to the entity.

2.2 The specific objectives for the Professional in pursuing these overall objectives are to understand and evaluate:

(a) the risks considered by the Auditee in collecting and storing DPD and the controls put in place in this regard.

(b) IS systems and procedures adopted by the Auditee to Protection the usage and sharing of DPD.

(c) Adequacy of measures put in place to be compliant with the provisions of laws and regulations, as applicable.

3.0 Requirements

3.1 The Professional shall agree with the Primary Stakeholder the nature and scope of the engagement to be undertaken, specifically that it relates to an audit of personal data of a digital nature and its proper protection as per the prevailing laws and regulations.

3.2 Professional shall have, or acquire, the knowledge and be familiar with the prevailing laws and regulations applicable to DPD of an Individual.

3.3 Professional shall understand the nature of the business of the auditee, extent of digitalization of business processes, the extent to which digital processes are outsourced, the requirements of collection of personal data for various business processes, the entire life cycle of personal data, governance of personal data etc.

3.4 Professional shall define the audit work procedure by understanding digital environment wherein the personal data is collected, processed or stored etc. Professional shall also understand the control over digital environment of the auditee to confirm whether the digital environment is owned by the auditee or outsourced to an external party. If outsourced, whether the data resides within the country or geography outside it.

3.5 Professional shall collect the information about the sharing of DPD to the Processor or to the outsourced vendor partner. Professional shall ensure whether the engagement mandate also requires to cover the audit of DPD at such vendor level. If it is not covered under the scope or if there are multiple vendors or third parties with whom the data is shared for different purposes, Professional shall seek an Independent Audit Report from such Processors, Third Parties or Vendors.

3.6 Professional shall define the audit work procedure to review the Service Level Agreements between the auditee and the Processors, Third Parties or Vendors to ensure appropriate clause is included in the agreements about the Protection of shared Digital Personal Data.

3.7 Professional shall have technical knowledge and competence to conduct the audit related to technology used for Collection, Processing, Storage, Modification etc. E.g. Profiling of Digital Personal Data, Setting up of Cookies on various platforms, Pseudonymisation, Anonymization etc. Professional may take the support of an Expert as per ISAS 220 covering "Using the Work of an Expert".

3.8 While Evaluation and Verification of Protection of Digital Personal Data is the key aspect of the engagement, Professional shall adopt specific work procedures to evaluate the measures, procedures and IS Controls adopted by the auditee to Protect the Digital Personal Data.

3.9 Professional shall define the work procedures to ensure the compliance of all the legal and regulatory provisions including the mechanism implemented by the Auditee to process the grievances related to breach of digital personal data.

3.10 Data Protection laws and regulations have recognized the Rights of an Individual in relation with digital personal data. Professional shall incorporate work procedures to ensure that auditee has taken appropriate steps to honour such rights.

4.0 Explanatory Comments

4.1 **Data Processing:** Data Processing includes operation or set of operations or function or set of function such as but not limited to Collection, Recording, Organization, Storing, alternation, use, transmission, sharing, making it available, destruction etc; which is performed on Digital Personal Data whether or not by digital means.

4.2 **Data Processor**: Data Processor is a Person who is Processing the Digital Personal data on behalf of auditee.

4.3 **Data Protection Related Laws & Regulations**: These are local area specific Laws or Regulations mandating the Protection of Digital Personal Data and recognising the rights of an individual related to it.

4.4 **Profiling of Digital Personal Data**: It refers to Digital Processing of Digital Personal Data, to identify and understand certain aspects related to Individual to analyse, predict, advertise etc such as Health, Individual Preferences, behaviour, likes and dislikes, areas of interest, locations, movements etc.

4.5 **Pseudonymisation:** It is a data processing technique that replaces individual identifiable information with artificial identifiers called pseudonyms, such as replacing a name with a unique ID number.

4.6 **Anonymization**: It is the process of removing or modifying Individually identifiable information from data so that it cannot be linked back to an individual, protecting their digital personal data.

5.0 Documentation of Work Procedures

5.1 An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows

5.1.1. Checklist to ensure the legal and regulatory provisions

5.1.2. Documentation of understanding the digital environment in which the digital personal data is processed.

5.1.3. Documentation of Digital Personal Data life cycle management.

5.1.4. Documentation of sharing or outsourcing of various functions, operations of the business and related Digital Personal Data

5.1.5. Communication regarding the Independent Assurance of Data Protection from Vendors, Third Parties or Processors.

5.1.6. If Auditee is not able to allow the copies of certain documents to be stored with Professional, the written communication about such restriction and references of such documents shall be maintained.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 440

CYBERSECURITY AUDIT

Contents

This Information Systems Audit Standard 440, on "Cybersecurity Audit," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or "Standard") establishes requirements for Cybersecurity audits.

1.2 **Definitions**: The following terms, along with their definitions, have been used in this Standard:

1.2.1 **Cybersecurity Audit** involves assessment of organisation's cybersecurity measures including governance, risk management, asset protection, detection, response, and recovery controls to safeguard information systems and data from threats, ensuring resilience, compliance, and operational continuity.

1.2.2 **Cybersecurity Controls** refer to the policies, procedures, technologies, and practices implemented to govern, protect, detect, respond to, and recover from cyber threats.

1.3 **Scope:** This Standard applies to all Information Systems (IS) audit engagements where cybersecurity controls are evaluated, whether as part of a specific cybersecurity audit or is integrated within other audits. It addresses diverse IT environments, including on-premises, cloud, hybrid, and emerging technologies, supporting objectives such as risk mitigation, regulatory compliance, and system resilience.

2.0 Objectives

2.1 The objectives of this standard are to:

(a) enable the Professional to form an opinion on the organisation's ability to manage cyber risks, with evidence and conclusions.

(b) ensure that the cybersecurity audits are performed as per the regulatory guidelines or cybersecurity frameworks, to the extent applicable.

(c) to enable the Professional in drawing conclusions on state of adequacy of cybersecurity posture of the organisation and its cyber-resilience.

3.0 Requirements

3.1 The Professional shall adopt a Risk Aligned Audit Methodology (RAAM) to plan and perform cybersecurity audit procedures, including review of the cybersecurity policies, risk management processes, and oversight mechanisms to ensure alignment with business context and threat landscape (refer Para 4.1).

3.2 The Professional shall document the nature, timing, and extent of cybersecurity audit activities, ensure reproducible records of governance assessments, asset inventories, control tests, detection reviews, response simulations, and recovery validations (refer Para 4.2).

3.3 The Professional shall evaluate the identification and classification of Information assets (systems, networks, data, applications), determining whether they are adequately inventoried, prioritised by criticality, and protected through layered defences such as perimeter security and access controls (refer Para 4.3).

3.4 The Professional shall test protective controls, including but not limited to, encryption for confidentiality, change detection for integrity, multi-factor authentication for access, and digital signatures for authenticity and non-repudiation, verifying their deployment and effectiveness across assets (refer Para 4.4).

3.5 The Professional shall assess detection capabilities, such as monitoring tools for anomaly identification, logging mechanisms for cyber threats, and alerting systems for real-time response, ensuring timely identification of potential incidents (refer Para 4.5).

3.6 The Professional shall examine response and recovery processes, including incident handling procedures, backup and restoration testing, and recovery time objectives, to confirm the organisation's ability to contain, eradicate, and recover from cyber events with minimal disruption (refer Para 4.6).

3.7 The Professional shall review third-party and supply chain risks, evaluating vendor security practices, contractual protections, and ongoing monitoring to ensure extended ecosystem resilience (refer Para 4.7).

4.0 Explanatory Comments

4.1 **Governance Assessment (refer para 3.1)**

Cybersecurity governance includes board level oversight, policy approval, and risk appetite definition. The Professional shall review minutes, policies, and risk registers to confirm alignment with evolving threats like ransomware or supply chain attacks.

4.2 **Asset Identification and Protection (refer para 3.2)**

Information Assets must be catalogued with criticality ratings to prioritise protection efforts. Layered defences including firewalls for perimeter protection, endpoint detection for insider threats, and data classification for targeted safeguarding, must be implemented proportionally to asset value and risk exposure, ensuring defence-in-depth and resource efficiency.

4.3 **Protective Controls Testing (refer para 3.3)**

Testing involves scanning for vulnerabilities, simulating attacks, and verifying encryption keys. Controls must be tested in production like environments to ensure real time effectiveness.

4.4 **Detection Capabilities (refer para 3.4)**

Detection relies on Security Information and Event Management (SIEM) systems for log correlation and Automated Tools and Techniques (ATT) driven anomaly detection. The Professional shall trace sample alerts from detection through investigation to measure response time and evaluate the effectiveness of escalation processes.

4.5 **Response and Recovery (refer para 3.5)**

Incident response procedures must address containment, eradication, and post-incident lessons learned. The Professional shall verify that recovery testing simulates full system outages to validate Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), ensuring alignment with business continuity requirements.

4.6 **Third-Party Risks (refer para 3.6)**

The Professional shall review vendor reports such as SRE 3402 or SA 402 of ICAI, service level agreements (SLAs), and penetration test results, while assessing right to audit clauses and shared responsibility models to ensure third party controls align with the auditee's cybersecurity risk posture.

4.7 **Audit Activity Documentation (refer para 3.7)**

The Professional shall ensure that records capture procedure details, evidence sources, and conclusions, enabling independent verification of cybersecurity audit outcomes and supporting reproducible, self-contained assurance.

5.0 Documentation of Work Procedures

An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.1 The Professional shall document cybersecurity audit procedures in a structured manner to support Cybersecurity Frameworks and demonstrate comfort level.

5.2 The Professional shall document:

5.2.1 CSF Function;

5.2.2 Threat scenario tested (e.g., ransomware, supply chain compromise);

5.2.3 Targeted control (e.g., SIEM rule, MFA policy, backup integrity check);

5.2.4 Risk-based selection (linked to CVSS score, or threat intelligence).

5.3 The Professional shall record,

5.3.1. Cybersecurity tools;

5.3.2. Attack simulation methods (e.g., phishing drills, privilege escalation testing);

5.3.3. Test environment (e.g., isolated sandbox, mirrored production);

5.3.4. Limitations (e.g., no live malware detonation, partial log access).

5.4 The Professional shall document,

5.4.1. Detection time (e.g., TTP observed in 12 mins via SIEM alert);

5.4.2. Containment effectiveness (e.g., lateral movement blocked at 3rd hop);

5.4.3. Recovery validation (e.g., RTO: 4 hrs, RPO: 15 mins achieved);

5.4.4. Comfort level assessment:

- Effectiveness: Control worked as designed
- Limitations: False positive rate 8%, no zero-day coverage

5.4.5. If the scope provides for then, Residual risk and recommendation (e.g., patch within 48 hrs).

5.5 The Professional shall ensure,

5.5.1. Cross-reference to Threat intelligence feed, Incident timeline, CSF Profile (Current vs. Target)

5.5.2. Secure retention with access logs and tamper-evident storage.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 510

REPORTING RESULTS

Contents

Paragraph(s)

This Information Systems Audit Standard 510, on "Reporting Results," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or "Standard") covers the responsibility of the Professional to have an effective communication of the results of the Information Systems (IS) audit with its stakeholders in the form of a written report. The IS audit report represents the culmination of the audit process and serves as the principal means by which the Professional conveys the results of the engagement to its intended users, including management, those charged with governance, and other specified stakeholders.

1.2 This Standard establishes the principles, requirements, and framework for the preparation, presentation, and issuance of IS audit reports.

1.3 **Definitions**: The following terms, along with their definitions, have been used in this Standard.

1.3.1 **Risk Rating** refers to a structured assessment and classification of the severity and likelihood of risk associated with an IS Audit finding, control deficiency, or identified vulnerability, typically expressed using a defined scale (such as Critical, High, Medium, Low) that reflects the potential impact on confidentiality, integrity, availability of information systems, business operations, regulatory compliance, or organisational objectives, and guides prioritisation of remediation efforts.

1.3.2 **Key Information Systems Audit Matters (KIAMs)** refers to those matters that, in the judgment of the Professional, were of most significance in the IS audit, including areas of higher assessed risk, significant judgments made during the audit, or matters that had a material effect on the audit approach or required specialised technical expertise to evaluate.

1.3.3 **Material Weakness** refers to a deficiency, or combination of deficiencies, in IS controls such that there is a reasonable possibility that a material misstatement, unauthorized access, data compromise, system failure, or non-compliance with critical requirements could occur and would not be prevented, detected, or corrected on a timely basis by the entity's control environment.

1.3.4 **Significant Deficiency** refers to a control deficiency, or combination of control deficiencies, in IS controls that is less severe than a material weakness, yet sufficiently important to merit attention by those charged with governance due to its potential impact on confidentiality, integrity, availability, reliability, or compliance.

1.3.5 **Control Deficiency** refers to a situation where an IS control is not designed, implemented, or operated in a manner that enables management or employees to prevent, detect, or correct on a timely basis, non-compliance with policies, security breaches, system failures, data integrity issues, or regulatory violations.

1.3.6 **Materiality** refers to determination of both quantitative factors (such as the cost of potential errors, volume of transactions affected, or regulatory penalty amounts) and qualitative factors (such as the criticality of affected systems, sensitivity of data at risk, pervasiveness of control failures, potential for fraud or security breaches, and reputational consequences), assessed in relation to the organisation's risk appetite, business objectives, and regulatory environment.

1.3.7 **Intended Users** refers to the parties for whom the IS Audit Report is prepared and to whom it is formally addressed or other specified recipients as identified in the engagement terms. These parties may include one or more of the following: Board of Directors, Audit Committee, Those Charged with Governance, Chief Information Officer (CIO), Chief Information Security Officer (CISO), senior management, regulatory authorities, external stakeholders, etc.

1.3.8 **Agreed-Upon Procedures (AUP) Engagement** refers to an Information Systems engagement in which the Professional performs specific procedures on IS subject matter as agreed upon by the Professional and the Primary Stakeholder, and reports factual findings without expressing an opinion or conclusion, where the users of the report form their own conclusions based on the procedures performed and results reported.

1.4 **Scope:** This Standard applies to all IS audit engagements conducted by or on behalf of an organisation, including but not limited to, internal audits, statutory audits, compliance audits, third-party assessments, cybersecurity audits, business continuity audits, and data protection audits relating to information systems, processes, controls, and technology infrastructure. The Standard is applicable regardless of the size, complexity, or technology environment of the entity, encompassing on-premises, cloud, hybrid, and emerging technology platforms.

2.0 Objectives

2.1 The objective of this Standard is to establish uniform principles and mandatory requirements for the preparation, presentation, and issuance of an IS audit report that is clear, comprehensive, consistent, structured, and provides reliable assurance to intended users regarding the effectiveness, adequacy, and operating performance of an organisation's IS, controls, governance mechanisms, risk management practices, and compliance with applicable requirements.

2.2 This Standard aims to ensure that IS audit reports effectively communicate the nature of assurance provided, the scope and objectives of the engagement, the audit procedures performed, significant findings and observations, identified deficiencies and their risk ratings, Key Information Systems Audit Matters (KIAMs), material weaknesses, significant deficiencies, audit recommendations, and where applicable, the Professional's conclusion or opinion.

3.0 Requirements

3.1 The Professional shall ensure that the IS Audit Report identifies the audit firm or internal audit department, the lead auditor(s) responsible for the report, the date of report issuance, to whom the report is formally addressed and (if applicable) an intended user (refer Para 4.1).

3.2 The Professional shall state in the IS Audit Report the specific IS processes, controls, technology domains, or subject matter covered by the audit, the period to which the audit procedures relate, and any boundaries, exclusions, constraints on scope, limitations on access to information, systems or personnel, or methodological limitations that may affect the nature or level of assurance provided.

3.3 The Professional shall include in the IS Audit Report a clear and explicit statement of management's responsibilities, acknowledging and confirming management's accountability for designing, implementing, and maintaining an effective IS environment with adequate governance, policies, procedures, and controls; establishing, monitoring, and evaluating internal controls including ITGCs and application controls; ensuring data integrity, completeness, accuracy, and protection; identifying, assessing, managing risks, including cybersecurity, privacy, continuity, and Operation Technology (OT) vulnerabilities, and implementing mitigations; ensuring compliance with laws, regulations, standards, contracts, and policies; providing unrestricted, timely access to systems, data, documentation, and personnel; overseeing third-party providers, cloud services, and outsourced functions; providing accurate written representations; and implementing timely remediation of deficiencies and recommendations (refer Para 4.2).

3.4 The Professional shall include the following while drafting the Report:

(a) a statement that the audit engagement and the Professional's work do not relieve management or those charged with governance of their responsibilities.

(b) an Executive Summary stating the overall IS Audit Opinion that represents the Professional conclusion on the effectiveness, adequacy, and operating performance of the information systems, controls, or subject matter examined within the defined scope of the engagement.

3.5 The Professional shall detail in the IS Audit Report the scope and methodology, IS Audit Findings, in a structured and consistent manner throughout the report. Where applicable, a specific section in the IS Audit Report addressing compliance with applicable regulatory and legal requirements.

3.6 Where applicable and material to the engagement, the Professional shall identify and communicate Key Information Systems Audit Matters (KIAMs) in the IS Audit Report, describing the nature of each matter, the reasons for its significance, and how it was addressed during the audit.

3.7 For Agreed-Upon Procedures (AUP) engagements, the Professional shall state this aspect in the IS Audit Report, describe the specific agreed procedures performed and resulting factual findings, and explicitly disclaim any opinion or conclusion, noting that users must form their own conclusions from the reported procedures and findings.

4.0 Explanatory Comments

4.1. **Identification of Auditor (Refer para 3.1):** Clear identification of the auditor, audit firm, report date, and intended recipients establishes accountability and ensures that the report is appropriately directed to those charged with governance and other stakeholders who have authority and responsibility to act on the audit findings. The report date signifies the point at which the auditor has completed all necessary audit procedures and obtained sufficient evidence to support the conclusions expressed.

4.2. **Responsibility of Auditee (refer para 3.3):** The Professional shall include in the IS Audit Report a clear and explicit statement of management's responsibilities that acknowledges and confirms management's accountability for:

(a) Designing, implementing, and maintaining an effective information systems environment, including adequate governance structures, policies, procedures, and controls over IT systems, processes, applications, infrastructure, and data;

(b) Establishing and maintaining appropriate internal controls over information systems, including IT general controls (ITGCs) and application controls, and regularly monitoring and evaluating the effectiveness of these controls;

(c) Ensuring the integrity, completeness, and accuracy of all data and information provided to the Professional, and preventing unauthorized access, alteration, or deletion of data within information systems;

(d) Identifying, assessing, and managing information systems-related risks, including cybersecurity threats, data privacy risks, business continuity risks, and operational technology vulnerabilities, and implementing appropriate risk mitigation measures;

(e) Ensuring compliance with all applicable laws, regulations, regulatory circulars, industry standards, contractual obligations, and internal policies relevant to information systems and technology operations;

(f) Providing the Professional with unrestricted and timely access to all relevant information systems, infrastructure, applications, network configurations, audit trails, source data, documentation, and personnel necessary to conduct the engagement;

(g) Overseeing and managing third-party service providers, cloud service arrangements, outsourced IT functions, and supply chain relationships to ensure they meet the organization's control, security, and compliance requirements;

(h) Providing written representations to confirm the accuracy and completeness of information and explanations provided during the engagement; and

(i) Implementing timely and effective remediation actions to address identified control deficiencies, material weaknesses, significant deficiencies, and audit recommendations.

4.3. Executive Summary and Audit Opinion (refer Para 3.4):

(a) Executive Summary shall highlight the most significant findings, material weaknesses, or Key Information Systems Audit Matters (KIAMs) identified during the audit, and communicate the principal risks and their potential business impact in clear, non-technical language that facilitates understanding by senior management and the board.

(b) The IS Audit Opinion shall be supported by the audit findings, control evaluations, risk assessments, and evidence obtained during the engagement, and shall clearly articulate the level of assurance provided using defined terminology that communicates the degree of effectiveness or the nature of deficiencies identified.

(c) Where an opinion is expressed, the Professional shall classify the opinion using clear and unambiguous terminology such as "Effective," "Effective with Exceptions," "Partially Effective," "Ineffective," or other appropriate descriptors that accurately reflect the overall state of controls and the assurance provided, consistent with the materiality and significance of identified deficiencies.

(d) Where the Professional is unable to obtain sufficient and appropriate evidence, or where material weaknesses or pervasive control deficiencies prevent the expression of an unqualified opinion, the Professional shall issue a qualified opinion, adverse opinion, or disclaimer of opinion, as appropriate, with clear explanation of the reasons and basis for the modification.

4.4. Audit Scope, Methodology and Findings (refer Para 3.5)

(a) The scope section shall define the specific IS domains, applications, infrastructure, processes, controls, and organisational units audited, identify any exclusions or limitations on the audit coverage, specify the period under review, and reference the applicable IS Control Framework used as the benchmark for evaluation.

(b) The methodology section shall describe the audit procedures performed, the testing techniques employed, the sampling methods applied where applicable, the nature and extent of system or control testing conducted, and the criteria used for evaluation of design effectiveness and operating effectiveness of controls.

(c) Each IS Audit Finding shall include a unique identifier, a clear and factual description of the condition observed, a statement of the applicable criteria or requirement against which the deviation was assessed, an evaluation of the root cause where determinable, an assessment of the potential risk or impact, the risk rating assigned, and the associated recommendation(s) for remediation.

(d) The Professional shall clear the potential risk or impact of each IS Audit Finding in terms of its effect on confidentiality, integrity, availability of information systems or data, operational disruption, financial loss, reputational damage, regulatory non-compliance, or other material consequences relevant to the organization's objectives and risk appetite.

(e) The Professional shall assign a risk rating to each IS Audit Finding based on a defined and consistent scale that reflects the severity and likelihood of the risk, enabling prioritisation of remediation actions by management.

(f) The Professional shall ensure that IS Audit Recommendations are actionable, specific, practical, and proportionate to the severity of the identified risk or deficiency.

(g) The Professional shall separately identify and report any material weaknesses or significant deficiencies in information systems controls discovered during the audit, including their nature, potential impact, and recommended corrective actions.

(h) The compliance section shall report on the organisation's adherence to applicable laws, regulatory circulars, directives, guidelines, industry standards, and internal policies relevant to IS, including but not limited to requirements issued by regulatory bodies such as RBI, SEBI, IRDA, CERT-In, or sectoral regulators, and shall identify any instances of non-compliance or partial compliance observed during the audit.

4.5. **Key Information Systems Audit Matters (KIAMs) (refer Para 3.6):** KIAMs represent those matters that required significant auditor attention, involved complex judgments, represented areas of heightened risk, or required specialized expertise to evaluate. Communication of KIAMs provides transparency about the focus of audit effort and the most challenging or significant aspects of the engagement, thereby enhancing the usefulness of the audit report for intended users.

4.6. **Agreed-Upon Procedures (AUP) engagements (refer Para 3.7):** In AUP engagements, the auditor performs specific procedures agreed upon with the engaging party but does not express an opinion or conclusion. The report must clearly state this distinction to prevent users from misinterpreting the factual findings as an assurance opinion. Users of AUP reports must form their own conclusions based on the procedures performed and results reported, and this responsibility must be clearly communicated.

5.0 Documentation of Work Procedures

An indicative list of the nature of documentation expected to demonstrate conformance to the Standard is as follows:

5.1 Report Header and Identification (Refer Para 3.1):

The Professional shall document:

(a) Final report headers confirming:
- Name of the audit firm or internal audit department.
- Name(s) of lead auditor(s) and engagement partner.
- Date of report issuance.
- List of intended recipients (addressee).

(b) Signed Report Approval Checklist confirming review and authorization prior to issuance.

(c) Distribution Log recording formal transmission (e.g., email, secure portal) to intended recipients.

5.2 Scope, Period, and Limitations (Refer Para 3.2):

This section shall cover:

(a) Scope clearly defining:
- Information systems, processes, controls, or technology domains audited.
- Audit period.
- Exclusions, boundaries, or constraints.

(b) Limitations detailing:
- Access restrictions (e.g., "Denied access to HR database logs").
- Methodological limitations (e.g., "Sampling applied; population > 1 million records").
- Impact on assurance level (e.g., "Limited assurance due to incomplete logs").

(c) Management Acknowledgement of scope and limitations, signed or emailed.

5.3 Management Responsibilities Statement (Refer Para 3.3):

The Professional shall document:

(a) Standard Management Responsibility Paragraph in the report, covering:
- Design, implementation, and maintenance of IS environment.
- GITCs, application controls, data integrity, risk management.
- Compliance, third-party oversight, access provision, representations.

(b) Management Representation Letter (MRL) on auditee letterhead, explicitly confirming all responsibilities listed in Para 4.3.

5.4 Executive Summary and Disclaimer (Refer Para 3.4):

This section of report shall cover:

(a) Executive Summary with:
- Overall IS Audit Opinion (e.g., "Effective", "Needs Improvement", "Ineffective").
- Basis for opinion.
- Key risks and recommendations.

(b) Standard Disclaimer stating:

"This audit engagement and the Professional's work do not relieve management or those charged with governance of their responsibilities."

5.5 Findings, Methodology, and Compliance (Refer Para 3.5):

The Professional shall document:

(a) Audit Methodology in the report, covering:
- Risk assessment approach.
- Sampling methodology.
- Testing procedures (walkthroughs, CAATs, interviews).

(b) Structured Findings (one row per finding) with:
- Finding ID

- Criteria
- Condition
- Cause
- Effect
- Risk Rating
- Recommendation (where applicable)
- Management Response (followup action or Action Taken Report (ATR).

(c) Regulatory Compliance (if applicable) mapping:

- Legal/regulatory requirement
- Control tested
- Test result
- Compliance status.

(d) Evidence Index linking each finding to work paper references.

5.6 Key Information Systems Audit Matters (KIAMs) (Refer Para 3.6):

The Professional shall, where ever appropriate, document:

(a) KIAM Identification for each matter, including:

- Description of the matter
- Reason for significance (e.g., "Material weakness in privileged access")
- Audit procedures performed
- Conclusion and impact on opinion

(b) Engagement Partner for inclusion of KIAMs in the report.

(c) Cross-reference to relevant findings and work papers.

5.7 Agreed-Upon Procedures (AUP) Reporting (Refer Para 3.7):

If the engagement is related to AUP:

(a) Engagement Letter clearly defining:

- Specific procedures agreed with the engaging party
- Factual findings only — no opinion.

(b) Report with:

- Statement: "This is an Agreed-Upon Procedures engagement"
- List of procedures performed
- Factual findings (no conclusions)
- Disclaimer: "Users of this report must draw their own conclusions"

(c) Link each procedure to its documented outcome.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).

ISAS EXPOSURE DRAFT
(1st Dec'25)

INFORMATION SYSTEMS AUDIT STANDARD

NO. 610

QUALITY MANAGEMENT AND CONTINUAL IMPROVEMENT

Contents

Paragraph(s)

This Information Systems Audit Standard 610, on "Quality Management and Continual Improvement," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Information Systems Audit Standards", the "Framework Governing Information Systems Audit Standards" and "Basic Principles of Information Systems Audit" issued by the Institute.

1.0 Introduction and Scope

1.1 This Information Systems Audit Standard (ISAS or “Standard”) deals with the responsibility of the Professional to ensure a consistent approach for an acceptable quality of work performed.

1.2 Quality as a general term is well understood, as is the fact that the Stakeholders are the best judges of acceptable quality. IS Audit engagements generally have multiple Stakeholders, and recognising their quality expectations is important in this respect. Delivering quality output requires a systematic and disciplined approach. This approach needs a combination of the right people, robust processes and a Quality Management and Continual Improvement System (QMCIS), regardless of the size of the organisation or budget.

1.3 **Scope:** This Standard applies to all Information Systems Audit (ISA) assignments.

2.0 Objectives

2.1 The objectives of this Standard are to ensure that:

(a) Quality Control requirements are in place and well understood.

(b) Work performed by the Professional and their staff follows a systematic and disciplined approach to achieve the quality control requirements.

2.2 The Standard also sets out the requirements in the areas of Quality Control Review (QCR) and Continuing Professional Education (CPE) which need to be adhered to by the Professional providing ISA services.

3.0 Requirements

3.1 The Professional shall establish a QMCIS designed to specify the quality control requirements and how these requirements will be met during all stages of an assignment (Refer Para 4.1).

3.2 The Professional shall ensure that assignments are appropriately staffed with individuals having relevant experience and technical capabilities. Since each assignment is unique in nature, and in order to keep-up with evolving trends, an ongoing Competency Development Plan (CDP) shall be put in place. (Refer Para 4.2).

3.3 The QMCIS shall be communicated and disseminated amongst all the staff working on the assignments and where appropriate, with the Experts engaged on the assignment. (Refer Para 4.3).

3.4 The Professional shall establish policies and procedures for QCR that sets out timely evaluation of the work performed before the report is issued (Refer Para 4.4).

3.5 A process to ensure regular monitoring of CPE requirements of the ICAI shall be implemented (Refer Para 4.5). Particularly, for the Professional conducting ISA engagements, at least 20 (twenty) of the annual CPE hours shall be in the area of ISA subjects.

4.0 Explanatory Comments

4.1 Quality Management and Continual Improvement System (refer Para 3.1):
The QMCIS shall consist of the quality control requirements and the policies and procedures which will ensure the compliance of these requirements. These would apply during all stages of an assignment. While the elements and components of the QMCIS depend on the best judgement of the Professional, these shall be designed to achieve certain essential objectives, as follows:

4.1.1 Before accepting the assignment:

(a) Independence of the Professional.
(b) Skills and competency of the Professional.
(c) Appropriateness of the scope and objectives of the engagement.

4.1.2 During execution of assignment:

(a) The objectivity of work performance, especially through application of hypothesis, where applicable.
(b) Processes for complying with applicable ISAS, especially regarding the review and supervision of
(c) quality of work performed (refer ISAS 350).
(d) Quality of evidence gathered and its linkage with conclusions drawn and reported.

4.1.3 Pre-completion of assignment:
An independent review of quality parameters, prior to report issuance.

4.1.4 Post-completion of assignment:

(a) An independent quality review of a sample of assignments.
(b) An independent "peer-review" type of mechanism to periodically (at least every alternate year) review the whole QMCIS.
(c) Continuously review and improve the QMCIS.

4.2 Staffing and Competency (refer Para 3.2):

Capabilities and competencies are developed through a variety of methods, including the following (indicative list):

(a) Professional education.
(b) Continuing professional development, including training programs.
(c) On-the-job work experience.
(d) Coaching of junior staff by more experienced professionals.

4.3 Communication of QMCIS (refer Para 3.3):

The quality control policies and procedures shall be documented and communicated to all Professionals and other staff (and, if appropriate, the Experts) working on the assignment. Such communication shall describe the quality control requirements, policies and procedures, and the objectives they are designed to achieve.

4.4 Quality Control Review (refer para 3.4):

4.4.1 A QCR is undertaken prior to the completion of the assignment by the Professional himself, or a Professional not involved with the assignment, who can be an internal reviewer as well as an external reviewer. This shall include but not limited to review of significant findings, evidence gathered, and conclusions reached in formulating the report. The QCR provides an opportunity to address any quality related concerns which may get highlighted at this stage.

4.4.2 **Internal Quality Reviews and Communicating the Results of the Internal Quality Review**

(a) The internal quality review framework should be designed with a view to provide reasonable assurance to that the IS audit engagement is able to efficiently and effectively achieve its objectives and scope.
(b) The internal quality review should be done by the person entrusted with the responsibility for the quality in IS audit and / or other experienced member(s) of the IS audit function.
(c) The internal quality reviews should be undertaken on an ongoing basis. The person entrusted with the responsibility for the quality in IS audit should ensure that recommendations resulting from the quality reviews for the improvements in the IS audit activity are promptly implemented.
(d) The person entrusted with the responsibility for the quality in IS audit should also ensure that the results of the internal quality reviews are also communicated to the appropriate levels of management and those charged with governance on a timely basis along with the proposed plan of action to address issues and concerns raised in the review report.

4.4.3 **External Quality Review and Communicating the Results of the External Quality Review**

(a) External quality review is a critical factor in ensuring and enhancing the quality of IS audit. The frequency of the external quality review should be based on a consideration of the factors such as the maturity level of the IS audit activity in the entity, results of the earlier IS audit quality reviews, feedbacks as to the usefulness of the IS audit activity from the customers of the IS audit, costs vis a vis perceived benefits of the frequent external reviews. The frequency should not in any case be less than once in three years.

(b) The external quality review should be done by a professionally qualified person having an in depth knowledge and experience of, inter alia, the professional Standards applicable to the IS auditors, the processes and procedures involved in the IS audit generally and those peculiar to the industry in which the entity is operating, etc. The external quality reviewer should be appointed in consultation with the person entrusted with the responsibility for the quality in IS audit, senior management and those charged with governance.

(c) The external quality reviewer should discuss his findings with the person entrusted with the responsibility for the quality in IS audit. His final report should contain his opinion on all the parameters of the IS audit activity and should be submitted to the person entrusted with the responsibility for the quality in IS audit and copies thereof be also sent to those charged with governance. The person entrusted with the responsibility for the quality in IS audit should, also submit to those charged with governance, a plan of action to address the issues and concerns raised by the external quality reviewers in review report.

4.5 **Continuing Professional Education (refer para 3.5):**

The Professional shall have in place a process to monitor the CPE compliance requirements and take necessary steps to:

(a) Develop plans to ensure timely completion of CPE programs during a set time-frame.

(b) Annually obtain written confirmation from everyone of compliance with CPE requirements.

5.0 Documentation of Work Procedures

5.1 An indicative list of the nature of documentation expected to demonstrate.

(a) Policies and procedures in the form of an QMCIS & QCR manual.

(b) Relevant correspondence, and communication documentation which evidences that sufficient quality control procedures were performed.

6.0 Effective Date

6.1 This Standard is applicable for all engagements beginning on or after … (a date to be notified by the Council of the ICAI).