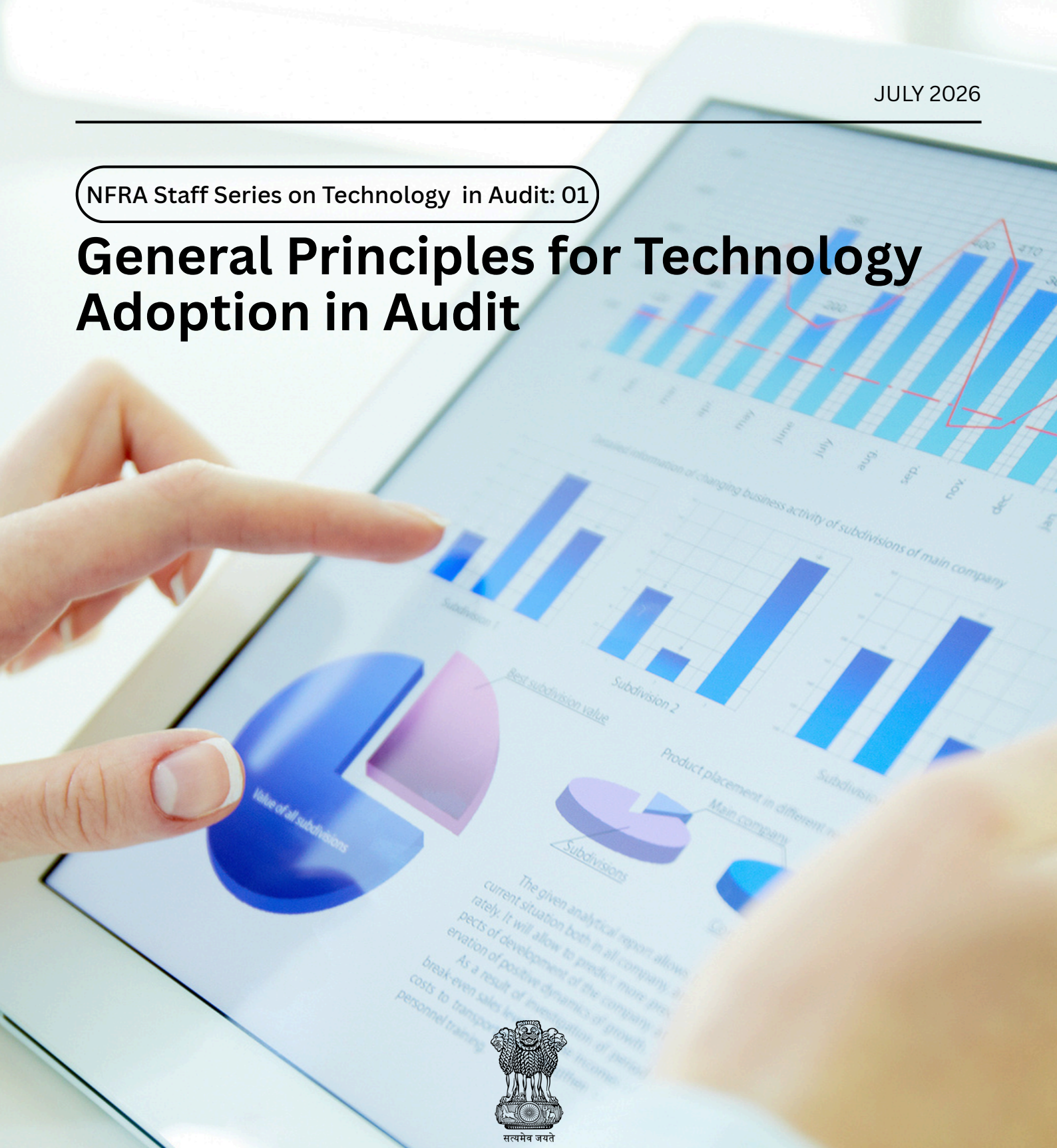
JULY 2026

NFRA Staff Series on Technology in Audit: 01

General Principles for Technology Adoption in Audit



सत्यमेव जयते

National Financial Reporting Authority

राष्ट्रीय वित्तीय रिपोर्टिंग प्राधिकरण

A. Introduction

Statutory audit is undergoing a significant shift in terms of technology adoption. Data analytics, automated tools and techniques (ATTs), and increasingly artificial intelligence (AI), including generative AI (GenAI) and agentic AI, are moving from being efficiency aids to core components of how risks are assessed, evidence is gathered and conclusions are reached. This shift offers genuine gains in audit efficiency through potential for entire population testing in place of sampling, faster and more consistent risk identification, and release of auditor's[1] time towards judgement-intensive areas. However, it also introduces risks that traditional audit methodology was not designed around- such as automation bias, opaque or non-deterministic outputs, model drift, data privacy exposure and the risk that reliance on technology may narrow rather than deepen professional scepticism.

This document, being the first in the NFRA Staff Series on Technology in Audit, sets out a principles-based framework, do's and don'ts and the changes to audit quality processes and systems within which statutory auditors of public interest entities need to evaluate, deploy and govern the use of technology, in the

[1] The terms 'auditor', 'audit firms' or 'firms' have been used interchangeably in this document

conduct of audits under the applicable Standards on Auditing (SAs). This initiative is in accordance with NFRA's obligations to suggest measures for improvement in overall audit quality and to promote awareness and significance of accounting and auditing standards, auditor's responsibilities, audit quality and such other matters.

The principles discussed in this document are not new. Each principle reiterates or clarifies an obligation that already exists under the Standards on Auditing, the Standards on Quality Control or the relevant ethical principles, and explains what that obligation means in the context of using technology rather than a manual process.

This document is technology-neutral and outcome-focused. The overall objective is to ensure that the audit opinion continues to rest on sufficient appropriate audit evidence, obtained and evaluated with unimpaired professional scepticism, under a system of quality control/management that has genuinely absorbed the risks that come with the technology in use.

B. Scope

The principles enumerated below cover technology used at any stage of the audit, planning and risk assessment, execution of substantive and controls testing, evaluation of evidence, and reporting and spans across conventional Computer Assisted Audit Techniques (CAATs) and data analytics through to machine learning, GenAI and Agentic AI.

These principles apply equally to tools developed in-house, tools licensed from third-party vendors, and tools embedded within a firm's or network firm's methodology.

B. General Principles

The 10 principles below apply irrespective of the specific technology in use and are intended to remain relevant even as tools evolve.

Principle 1: Technology neutrality, principles-based application

The Standards on Auditing have always been technology-neutral, for example, SA 500 requires evaluation of whether evidence is sufficient and appropriate and not how it was generated. In keeping with the same, the expectations articulated herein are outcome-based, focusing on the sufficiency and appropriateness of audit evidence, the quality of risk assessment and the integrity of the audit opinion, without prescribing the technology to be used in achieving those outcomes. This principle neither mandates nor prohibits the use of any specific tool, vendor or technique. However, the auditor cannot treat the usage of a tool as a substitute for meeting the requirements of any underlying standards.

Principle 2: Non-delegable auditor responsibility

The responsibility for the audit opinion remains with the auditor,

irrespective of the sophistication of the tools used. Technology may inform and accelerate professional judgement; however, it cannot be a substitute for it and cannot be invoked to explain away an inappropriate conclusion. The audit report is signed by, and the opinion belongs to, an identified auditor and not to any technology or tool that has assisted in reaching it.

Principle 3: Audit evidence standards apply regardless of source

Output from an ATT can be considered as audit evidence, or an input to it, only once its relevance and reliability have been evaluated by the auditor in the same manner as applicable for any other source which is understanding the source, assessing the risk of manipulation or error, and testing accordingly. There is no separate, lower evidentiary bar for technology-generated information; the same standard governs, applied with judgement to the circumstances of the tool in question.

Principle 4: Professional scepticism must be actively preserved

Fluent and well-presented machine output is likely to invite automation bias which is the tendency to accept plausible-looking results with less challenge than a human-prepared equivalent would receive. Engagement teams and reviewers must consciously counter this tendency. Technology cannot be expected to exercise professional scepticism on the auditor's behalf; it must be exercised by the person relying on the output, regardless of how convincing that output appears.

Principle 5: Risk-based, proportionate governance

The requirements of validation, certification and review of a tool need to be applied in proportion to the risk it poses to audit quality and may not be required to be applied uniformly across all tools. For example, a translation aid and an agentic tool that selects and tests samples do not warrant the same intensity of validation. Treating them identically may overburden usage of low-risk tools or under-scrutinise the tool which carries a high-risk. This is an application of the risk-based approach to quality control/management that the standards already require of a firm's system as a whole.

Principle 6: Explainability commensurate with materiality

The extent of explainability and documentation with respect to any output generated using a tool, needs to be proportionate with how material the output is to the audit opinion. This follows from the existing requirements of SA 500 with respect to reliability and documentation under SA 230. These standards require a level of understanding and documentation proportionate to the matter under consideration. This principle differs from Principle 5 since Principle 5 governs how much a firm invests in validating and certifying a tool before it is approved for use whereas

Principle 6 governs how much an auditor needs to understand and document about a specific output, once the tool has been used, given what that output is being relied on for on this particular engagement. A high-risk tool under Principle 5 may not automatically produce a material output under Principle 6, and a low-risk tool is not exempted from this principle merely because it subject to lower governance requirements as per the firm's quality control policies.

Principle 7: Governance needs to precede deployment

A firm's system of quality control is expected to treat technology as a resource whose risks are identified and addressed before deployment, in the same way it would treat any other resource on which the quality of an engagement depends. Tools must be validated and approved in accordance with the firm's policies, before they are used on a live engagement and not evaluated retrospectively. The firm needs to ensure that the tool operates as designed and achieves the purpose for which it is intended and the outputs achieve the purpose for which they will be used. Further, any material changes to a tool such as model updates, new data source, vendor change (not an exhaustive list) would lead to a re-validation of the tool. Validation of the tool, prior to implementation, cannot be considered as the basis for continued reliability.

Principle 8: Data stewardship

Client and personal data processed by or through any technology tool must be

protected in a manner that is consistent with the firm's confidentiality obligations under the relevant ethical principles, the Digital Personal Data Protection Act, 2023, and any other applicable sectoral requirements. These obligations exist independently of the tool used to process the data. A firm cannot rely on a vendor's terms of service (without validation) or on the convenience of a tool, as a substitute for its own responsibility to protect client and personal information.

Principle 9: Transparency requirements

Where technology use is material to the audit approach, the auditor need to be able to explain such use. This is in accordance with the auditor's obligations under SA 260 and SA 265, which require the auditor to explain the audit strategy and audit approach to those charge with governance.

Principle 10: Continuous monitoring, not one-time approval

Approval of a tool before deployment is only a starting point and not a complete exercise by itself. Given the adaptive and non-deterministic nature of outputs (the same input can

produce a different result on a different occasion) and velocity of changes in the underlying technologies, auditors must monitor performance across the tool's working life and re-approve the tool when warranted, rather than relying indefinitely on an initial approval. This reflects the ongoing monitoring obligation that are applicable on the firm's system as a whole.

D. General Do's and Don'ts in the Use of Audit Technology

These apply to all forms of audit technology data analytics, CAATs and ATTs:

Do's:

- Validate the completeness and accuracy of data before it is fed into any analytics or testing tool.
- Test IT general controls over the systems from which data is extracted, as a precondition to relying on the extraction.
- Document why a particular tool was selected for a particular procedure and retain the tool version and configuration used.
- Evaluate the service organisation controls (e.g., SOC-type reports) of any cloud-based or third-party-hosted tool.
- Evaluate the logic behind any risk-scoring or exception-flagging performed by a tool and not merely its output.
- Retain an audit trail sufficient for an experienced auditor unconnected with the engagement to understand what the tool did.

Donts:

- Treat full-population testing by a tool as eliminating the need for a substantive risk assessment.
- Use unvalidated or locally-built spreadsheets, macros or scripts on live engagements without firm-level approval.
- Accept a tool's classification of items as "low risk" without periodically testing that classification.
- Rely on vendor claims about a tool's accuracy or reliability without independent evaluation by the firm.
- Change a tool's configuration or data source mid-engagement without re-assessing its impact on planned procedures.
- Allow an efficiency gain from technology to compress the time available for review and challenge.

E.Changes to Processes and Systems

Adopting technology requires auditors and audit firms to make identifiable changes to how they govern quality, document work, train staff and monitor performance. The requirement below are expected to be evidenced, not merely asserted:

- Systems of quality control/management: Quality systems need to explicitly identify technology use as a distinct risk area within the risk assessment process, with defined risk responses and not folded generically into "resources".

- Tool certification and validation lifecycle: A formal pre-deployment testing, approval and phased roll-out process, followed by ongoing monitoring and defined re-approval triggers such as a material model update, an observed performance issue, or a change in regulatory guidance.
- Structured, inspectable documentation: Audit documentation practices need to move toward a standardised structure that makes technology assisted work traceable in terms of which tool was used to process a specific balance or assertion, and what was extent of human review on such processed output.
- Training and competence: Technology literacy embedded in continuing professional development, differentiated by role on the engagement - preparers (safe and effective use), reviewers (critical evaluation and bias awareness), and engagement partners (governance and disclosure judgement).
- Monitoring and internal inspection: Root-cause analysis of technology-related findings need to feed into any annual system of quality management evaluation, with trends reported to leadership.
- Third-party and vendor oversight: Contracts with technology vendors need to address data protection, intellectual property, access to explainability documentation, audit rights, and business continuity, with particular attention where a tool is built on a foundation model outside the firm's direct control. Where a tool is provided and centrally contracted by a network or a common technology platform, the obligation is to satisfy and be able to demonstrate, that network-level due diligence and contractual protections meet the substance of this paragraph.
- Change management: Version control and internal communication needs to be ensured whenever a material update to a tool could change its behaviour.

F. Data Privacy, Cybersecurity and Confidentiality

This document relates to risks that technology poses to audit quality. It does not displace an auditor's/audit firm's independent obligations to ensure that any technology or AI tool complies with the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000 and its reasonable security practice requirements, and any applicable sectoral requirements of other Regulators in respect of audit clients they regulate. The auditor/audit firm needs to maintain an appropriate information security framework covering cloud-hosted and third-party tools, with particular attention to cross-border data transfer where a vendor's infrastructure or model is hosted outside India.

G.Ethics and Independence Considerations

Confidentiality: Use of any tool must not result in client information being processed or retained outside the auditor's or audit firm's controlled environment, consistent with the technology-related ethical principles.

Automation bias as an ethical concern and not merely a quality issue: Indiscriminate or over reliance on machine-generated outputs, even when they appear credible, may amount to a failure to exercise the fundamental principles of professional competence, judgment and due care. Consequently, auditors and audit firms need to follow the fundamental principles applicable to the profession in using technology.

Disclaimer:

1. *This document by NFRA Staff is intended purely towards promotion of awareness of auditing standards and audit quality as part of NFRA's education, training, seminar and advocacy initiatives. NFRA does not accept any responsibility or liability for any loss caused to any person or any entity, howsoever arising from the use of or refraining from the use of the contents of this document.*
2. *The above principles are supplementary to and do not override the Standards on Auditing, the Standards on Quality Control or relevant ethical principles; it must be read together with them. This document is not a policy or standard or recommendation or statement of Executive Body of NFRA, of the Authority, or of the Government and is not issued as a substitute for any obligations of Auditors or Audit firms, as are provided in law, rules, and regulations.*