1st DRAFT (16 Nov'20)
FOR REVIEW BY SG
(On XX Nov'20)

The Digital Accounting and Assurance Board (DAAB) of The Institute of Chartered Accountants of India (ICAI) invites comments on a new Forensic Accounting and Investigation Standard (FAIS) on – **Evidence Discovery in Digital Domain**.

Comments are most helpful if they indicate a clear rationale and, where applicable, provide a suggestion for alternative wording.

Comments can be Submitted at
https://forms.office.com/Pages/ResponsePage.aspx?id=DOHFOzhjoU6NJ-O1tggEOvuF6SRz25pIvVExBjm2K8JUQlkzNTFWWElQWDVKWEgwR0FWOTRPRUtZQi4u

Last date for sending comments is January 28**, 2020~~1~~1.**

FORENSIC ACCOUNTING AND INVESTIGATION STANDARD NO. 520

EVIDENCE DISCOVERY IN DIGITAL DOMAIN

Contents

This Forensic Accounting and Investigation Standard Number 520, on "Evidence Discovery in Digital Domain," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to the Forensic Accounting and Investigation Standards", the "Framework Governing Forensic Accounting and Investigation Standards" and "Basic Principles of Forensic Accounting and Investigations" issued by the ICAI.

1 Introduction and Scope

1.1 As most business activities and transactions shift to the Digital Domain (DD), the evidential matter now required to complete Forensic Accounting and Investigations (FAI) assignments has to be discovered in a new way, referred to as "electronic discovery (or e-discovery)".

1.2 The Professional is expected to have, or acquire, the expertise necessary to undertake e-discovery and conduct assignments in the DD. Moreover, technical nuances of this domain hinder easy access to the evidence and unique skills and challenges come into play when conducting these assignments.

1.3 **Definitions:**

(a) **Digital Domain:** The electronic environment where Digital Evidence is present, is referred to as the Digital Domain. This may be in the form of Information Systems (IS) used by an organisation or Cyberspace (which includes the communication network connecting the organisation's IS to the Internet and rest of the domain).

(b) **Digital Evidence:** The term refers to data or information used as evidence, and is created, converted, recorded, stored, accessed, processed, examined, transmitted or used in electronic form. To ensure that digital evidence is admissible in a court of law, it needs to comply with certain legal conditions and Chain of Custody.

(c) **Electronic (e-) Discovery:** The process used for gathering and collecting evidence in the Digital Domain, which is to be used by a Professional conducting an FIA assignment or by parties other than the Professional in legal proceedings.

(d) **Digital Chain of Custody:** Digital Evidence which can be demonstrated to have been procured, secured, studied, analysed and stored in its original digital form and moved from one location (or custody) at some point in time to another at some other point in time, without being tampered or altered in any way or form during the move.

1.4 **Scope:** This standard applies to all FAI assignments which relay on the need to discover digital evidence to complete the work procedures in the Digital Domain.

2 Objectives

2.1 This Standard on Evidence Discovery in the Digital Domain aims to establish the essential practices to be followed by the Professional in e-discovery, as part of the work procedures required to perform effective FAI assignments.

2.2 The supporting objectives of the Standard are as follows:

(a) To familiarise the Professional with the nature of e-discovery and how it is undertaken.
(b) To consider the unique risk factors and limitations and the steps required to mitigate or manage those situations.
(c) Outline certain essential procedures to be followed in e-discovery of evidence.
(d) Evaluate the resources, skill and timeline required for evidence discovery in the DD.

3 Requirements

3.1 The Professional working in the digital domain shall maintain and deploy a documented process for e-discovery of evidence, stipulating relevant technical standards to be followed in this regard (refer Para 4.1).

3.2 The Professional shall undertake an overall understanding of the prevalent Information Systems (IS) environment and its linkage to the Digital Domain in so far as it is relevant to the assignment objectives (refer Para 4.2).

3.3 Discovery and gathering of evidence in the Digital Domain shall be conducted by those who have the requisite skills, expertise and experience of working in such a domain so as to preserve the reliability and admissibility of digital evidence in a court of law (refer Para 4.3).

3.4 Evidence gathered in the Digital Domain shall comply with the national laws (or the International laws, where applicable) concerning the Digital Domain and respective data privacy laws which place restrictions on the e-discovery and custody of digital evidence (refer Para 4.4).

3.5 Where necessary, the Professional shall deploy appropriate forensic tools to authenticate the evidence and maintain a reliable chain of custody over the evidence (refer Para 4.5).

4 Explanatory Comments

4.1. **E-Discovery Process (refer Para 3.1):** The Professional shall undertake work in the Digital Domain through a laid down process which takes into account the best practices in the domain. Some of the essential content of the process documentation is as follows (indicative list):

(a) The specialised skills, expertise and qualifications required to conduct the technical work procedures in the DD, particularly for e-Discovery and custody.

(b) Identification of data requirements in line with the assignment objectives and the hypotheses under consideration to shortlist the data needs.

(c) Procedures to identify data sources and the manner of accessing the same, including requirement of digital tools to be employed for e-Discovery.

(d) Technical Standards to be deployed in undertaking the work procedures, requirements based on technical literature, such as the following:

(i) Diploma in Information System Audit (DISA)

(ii) Certified Information Systems Auditor (CISA)

(iii) IS Audit and Assurance Standards issued by ISACA.

(iv) ISO/IEC 27000 series on IT- Security Techniques.

(v) Best Practices for Digital Evidence Collection issued by Scientific Working Group on Digital Evidence (SWGDE).

(vi) ISO/IEC 27050 series on IT- Electronic Discovery.

(vii) Forensic Examination of Digital Evidence issued by the US National Institute of Justice (NIJ).

(e) Summary of the relevant laws and regulations applicable to IS assignments and e-discovery and digital custody in particular.

(f) Nature of work records and documentation to be maintained to support the work performed and the summary of findings.

4.2. **Understanding the Digital Domain (refer Para 3.2):** The professional shall undertake a brief review of the IS environment and understand the elements of the domain which may be relevant to plan and execute the assignment. The following steps may be considered for this exercise (indicative list):

(a) The extent to which the IS environment is used to record, compile, process and analyse the information.

(b) The IS architecture, the hardware and various applications being used, their interaction with the external environment, and general understanding of the whole set-up.

(c) Overview of the governance structure in place, the policies and procedures deployed and an outline of the controls in place with past control compliance history (if any).

(d) The significance and complexity of digital processing, the extent of insourcing vs. outsourcing of IS activities and the use of external (third party) resources to oversee the secure processing and storage of data and information.

(e) Summary of any risk assessment undertaken, nature of vulnerabilities identified, and risk mitigation steps implemented.

4.3. **Qualified Expert (refer Para 3.3):** Based on the needs of the assignment, the Professional shall use his best judgement to establish the sufficiency of credentials of the person conducting e-discovery. This determination may result in the need to temporarily acquire technical experts for the assignment, in line with FAIS 230 on "Using the work of an Expert".

Where assignment output may be subject to cross-examination in a court of law, formal qualifications and extensive experience of the expert may be essential. Conversely, evidence to be used in an internal inquiry may only require certain basic skills by the person conducting e-discovery. Irrespective of the credentials, the expert is expected to have an understanding of the need to safeguard the evidential matter to maintain its original form, hence reliability.

4.4. **Compliance with Laws & Regulations (refer Para 3.4):** It is essential to follow Statutory requirements during the process of discovery of digital evidence due to the unique risks in the DD. Certain laws specific to this, prevalent in India, are the Information Technology Act, 2000, the Indian Evidence Act 1872, and Personal Data Protection Bill, 2019. The General Data Protection Regulations (GDPR) of the European Union may also be applicable in some cases.

4.5. **Forensic Tools (refer Para 3.5):** Working in the DD to discover digital evidence requires the use of certain digital (software) tools. The Professional (or Expert) is expected to recognise the best tool for the situation and ensure that the tool being deployed is most appropriate for the purpose.

5 Documentation for Compliance

5.1 The Digital Domain Process Manual shall be maintained as indicated under para 4.1 above, the content of which shall include all the unique procedures which need to be performed in the DD.

5.2 The assignment documentation shall include the chain of custody information for all the evidence gathered. This could be an electronic chain of custody which can be tested and relied upon independently with logs etc. This may include adequate backup procedures in the form of location custody, indexing, labelling, header to each activity and files, organised folders, password protected secure access, the system user identity of personnel, encrypted, sealed, version descriptions, etc.

5.3 Date and time stamps as suitable for testimony and evidence in a court of law or representation to stakeholders or competent authorities, as per the mandate

without infringement of the Evidence Act and applicable Information Technology Regulations.

6 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).