The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

TRANSITIONING TO DIGITAL EVIDENCE MANAGEMENT UNDER SECTION 63 OF THE BHARATIYA SAKSHYA ADHINIYAM, 2023: AN EMPIRICAL ASSESSMENT OF JUDICIAL ADMINISTRATION AND READINESS IN THE DISTRICT & HIGH COURT OF BILASPUR, CHHATTISGARH

~ Dr. Dharmendra Sharma

Abstract

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) sets out more technical requirements for proving electronic records, including a prescribed certificate, hash particulars and an expert component. Meeting those requirements depends on administrative systems that preserve an item's identity from acquisition through filing, hearing and archive. This article examines publicly documented readiness in Bilaspur, Chhattisgarh, through a bounded audit of statutes, state rules, court-preservation instruments, official e-Courts reports and relevant decisions available through 31 October 2026. It compares the BSA certificate with Chhattisgarh's 2020 online e-filing rules, its 2025 eSakshya Management Rules, digital-preservation arrangements and the reported launch of a paperless court and e-Malkhana in Bilaspur. The reviewed documents show substantial digital infrastructure, but no publicly documented item-level protocol that links acquisition, registry receipt and archive integrity events with Part A/Part B certificates, system identifiers, access logs and appellate retention. The article proposes a court-led SOP and pilot indicators. No Bilaspur case files, system logs, interviews or survey data were available. The findings therefore concern public documentation, not actual error rates or system performance.

Keywords: Bharatiya Sakshya Adhiniyam; Section 63; electronic evidence; hash value; eSakshya; court administration; Chhattisgarh; Bilaspur; digital preservation; standard operating procedure

1. Introduction

Since 1 July 2024, the BSA has recognised electronic records and prescribed how computer output may be proved. Sections 61–63 address legal effect, proof of contents and certification. The administrative question is whether a court can identify and verify a file's source, production method, device details, hash and certificates at each stage from capture through filing, hearing and appeal.1

The study covers Bilaspur District and Sessions Court and the High Court of Chhattisgarh at Bilaspur. Relevant institutional layers include online filing rules, police-facing eSakshya rules, national preservation guidance and state digitisation initiatives. In December 2025, official e-Committee reporting noted the launch of Bilaspur's first paperless court and e-Malkhana. These initiatives signal investment in digital infrastructure. They do not establish that every file tendered in court has complete certificate, hash and custody data, or that those data are interoperable.2, 3

The central question is whether published rules make the hand-offs auditable. Section 63(4) requires a prescribed certificate with each submission for admission, and its Schedule calls for information from both a responsible party and an expert. Separately, Chhattisgarh's published 2020 e-filing rules direct an Administrator to generate a hash when an online filing includes audio or video. The 2025 eSakshya Rules prescribe secure event packets, unique identifiers, hash values, immutable storage and an app-generated Part A certificate. These controls apply at

[1] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63, India Code, https://www.indiacode.nic.in/bitstream/123456789/20063/1/a2023-47.pdf (last visited Oct. 31, 2026).
[2] e-Committee, Supreme Court of India, e-Initiatives—Chhattisgarh, https://ecommitteesci.gov.in/project/e-initiatives-cg/ (last visited Oct. 31, 2026). The page reports hybrid proceedings, e-filing in District and Sessions Courts, ICJS integration, e-Sewa initiatives, and judicial training.
[3] e-Committee, Supreme Court of India, e-Committee Newsletter, Dec. 2025, at 18–19, https://cdnbbsr.s3waas.gov.in/s3ec04e91068fff3d7fa1594dfdf3b4308/uploads/2026/04/2026042576.pdf (reporting the launch of Bilaspur District & Sessions Court's first paperless court and e-Malkhana on Dec. 15, 2025).

different stages under different instruments. A hash recorded at one stage should not be assumed to satisfy a requirement at another.[4, 5, 6]

This article maps Bilaspur's controls across capture, filing and preservation. It distinguishes acquisition, receipt and archive checkpoints, then proposes an SOP that connects the existing systems. The paper recognises recent general scholarship on Section 63 and contributes a local crosswalk among Chhattisgarh's rules.[7]

2. Legal and Institutional Framework

2.1 The BSA certificate and transition rule

Section 61 recognises the legal effect of electronic or digital records, subject to Section 63. Section 62 requires their contents to be proved under Section 63. Under Section 63(4), the prescribed certificate must accompany the record each time it is submitted for admission. It identifies the record, explains how it was produced, gives particulars of the relevant device or system, and addresses the statutory operating conditions. The Schedule divides the required information between Part A, completed by the person in charge of the device or relevant activities, and Part B, completed by an expert. It also requires hash values and a hash report. A hash is useful only when the record identifies the object, algorithm, time, tool and custodian. The value alone does not establish authorship, completeness, lawful collection or truth.[8]

The identity and eligibility of the Part B expert require careful treatment. Section 39 of the BSA and Section 79A of the Information Technology Act provide relevant statutory context, but the BSA Schedule does not expressly restrict Part B to a person notified under Section 79A. In May 2026, the Supreme Court upheld the constitutionality of hash and expert certification under Section 63(4). It held that the Madras High Court's Section 79A-only view was not binding and observed that a person with special skill in computer science and cyber forensics may qualify if

[4] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(4) & Schedule. Section 63(4) requires the prescribed certificate to accompany the electronic record at each instance of submission for admission; the Schedule divides certificate particulars between the responsible party (Part A) and an expert (Part B).
[5] High Court of Chhattisgarh, Rules for Online Electronic Filing, Notification No. 6102/Rules/2020, rr. 1, 8.4 (July 10, 2020), https://highcourt.cg.gov.in/information/rule/2020/noti_6102_10072020.pdf.
[6] Chhattisgarh eSakshya Management Rules, 2025, Notification No. ESTB/1255/2025-Home Section, rr. 2(g), 3 (Apr. 19, 2025), https://highcourt.cg.gov.in/information/rule/2025/eSakshya_Management_Rules_2025.pdf.
[7] M. Suhail Salafi, Admissibility of Electronic Records under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: Practical Challenges before Trial Courts, 4(1) Int'l J.L. Res. & Legal Metrics (Oct. 16, 2026), https://doi.org/10.5281/zenodo.23408894.
[8] See supra note 4.

the court is satisfied on unimpeachable material. The Court left the question of law open and gave no conclusive ruling on expert qualifications. A local SOP may set a verification and escalation process, but it cannot turn a disputed technical opinion into a conclusive admissibility ruling.[9, 10]

The transition date also affects which evidentiary law applies. Section 170(2) preserves proceedings pending immediately before commencement under the former Indian Evidence Act, 1872. A record tendered after 1 July 2024 in a proceeding already pending on 30 June 2024 should therefore not be routed automatically under BSA Section 63. The saving clause and relevant procedural orders must first be considered. In May 2026, the Chhattisgarh High Court considered an interim challenge in a 2021 Negotiable Instruments Act complaint after the trial court rejected an application to file a certificate late. The High Court issued notice and interim relief. It did not decide the BSA's temporal application or establish a general rule allowing late certificates. The order illustrates a transition question; it is not a settled holding on that issue.[11, 12]

2.2 Chhattisgarh's filing, capture and preservation instruments

The Chhattisgarh High Court's published Rules for Online Electronic Filing apply to the High Court, District Courts and tribunals. Under Rule 8.4, when an online filing includes audio or video, the Administrator must generate a hash value. This creates a court-side integrity check at filing. The rule does not say that the receipt hash replaces the BSA Schedule certificate or the hash generated during evidence capture. Rule 10.1 provides for preserving originals of scanned and digitally signed documents for production or inspection as the Bench may direct. Rule 10.2 requires signed vakalatnamas, signed and attested affidavits, and other documents whose

[9] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 39; Information Technology Act, No. 21 of 2000, § 79A. Section 63 and the Schedule should be read with the Act's expert-opinion provisions; the statute does not make every Part B signatory a Section 79A examiner by express text.

[10] Pune Bar Ass'n v. Union of India, W.P. (C) No. 599/2026, 2026 SCC OnLine SC 1297 (May 22, 2026). The Court upheld the constitutionality of hash and expert certification under § 63(4). It held that the Madras High Court's view limiting Part B to an examiner notified under § 79A was not binding and observed that another person with special skill in computer science and cyber forensics may qualify if the court is satisfied on unimpeachable material. The Court left the question of law open and gave no conclusive opinion on expert qualifications.

[11] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 170(2); Ministry of Home Affairs, S.O. 849(E), Gazette of India, Extraordinary, pt. II, sec. 3(ii) (Feb. 23, 2024) (appointing July 1, 2024 as commencement date, except as specified).

[12] Vineet Fules v. Saiyyad Mohsin Ali @ Juganu, W.P. (227) No. 570/2026 (Chhattisgarh High Court May 11, 2026) (interim order). The matter concerned a 2021 complaint and a rejected late certificate application; the High Court issued notice and interim relief, not a final ruling on the temporal application of the BSA or late certification.

authenticity is likely to be questioned to be preserved for at least two years after final disposal; final disposal includes disposal by a superior appellate court. Rule 12 recognises privacy and confidentiality exceptions. The High Court rules index lists a 2021 amendment, but its substantive text was not available in the materials reviewed. This article therefore treats the published 2020 wording as the documented baseline and recommends confirming the consolidated current text before adoption.[13, 14, 15, 16]

The Chhattisgarh eSakshya Management Rules, 2025 set out a police-to-court route for material captured through the application. An event packet includes a unique 16-digit SID, opening and closing timestamps, and geolocation. The SID and its contents receive a unique hash and are stored in immutable storage. The Rules direct investigating officers to record specified search, seizure and investigative material through the app. They provide for an app-generated, electronically signed Part A certificate, link the SID to FIR/general-diary data in CCTNS, and allow court access through CIS/Sakshya Portal on ICJS. Rule 11 states that the Rules supplement other applicable law. The published text supplies important capture and routing controls, but does not explain how the Part B expert certificate is obtained, how a registry receipt hash is reconciled with the event-packet hash, or how every independently sourced record is handled. These are matters for an operational crosswalk; they do not establish that a live system lacks a function.[17, 18, 19]

[13] See supra note 5.
[14] High Court of Chhattisgarh, Rules for Online Electronic Filing, Notification No. 6102/Rules/2020, rr. 8.4, 8.7 (July 10, 2020). Rule 8.4 addresses hashing of audio/video in an online filing; it does not specify reconciliation with an eSakshya acquisition hash.
[15] High Court of Chhattisgarh, Rules for Online Electronic Filing, Notification No. 6102/Rules/2020, rr. 10.1, 10.2, 12 (July 10, 2020). Rule 10.1 provides for preservation of originals of scanned and digitally signed documents for production or inspection as the Bench may direct. Rule 10.2 requires specified signed documents and documents whose authenticity is likely to be questioned to be preserved for at least two years after final disposal, including disposal by a superior appellate court. Rule 12 recognises confidentiality and privacy exceptions.
[16] High Court of Chhattisgarh, Rules for Online Electronic Filing, Notification No. 6102/Rules/2020, official rules index (listing Amendment Notification No. 6894/Rules/2021 dated July 16, 2021). The amendment's substantive text was not available in the public materials examined; references here are to the published 2020 text and are subject to confirmation against the consolidated current rules.
[17] See supra note 6.
[18] Chhattisgarh eSakshya Management Rules, 2025, Notification No. ESTB/1255/2025-Home Section, rr. 4–11 (Apr. 19, 2025). Rule 4 provides an app-generated Part A certificate and e-signature; Rules 5–7 address FIR/general-diary linkage, forwarding and court access through CIS/Sakshya Portal on ICJS; Rule 11 makes the Rules supplementary to other applicable law.
[19] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63 & Schedule; Chhattisgarh eSakshya Management Rules, 2025, rr. 4, 11.

The e-Committee's Digital Preservation SOP predates the BSA. It addresses digitisation, storage, retrieval, preservation metadata, access controls, timestamped logs and transfer tracking, and provides a useful foundation for records management. It is not, by itself, a current Section 63 intake manual for live evidence. Its references and design predate the BSA, and its main focus is court digitisation and long-term preservation. The Supreme Court's 2023 directions in Jitendra Kumar Rode also treat record digitisation and preservation as administrative responsibilities involving Registrar Generals and District Judges. The Chhattisgarh High Court index separately lists a 2025 SOP on digital preservation of High Court and District Court records. Because its underlying text was not available for verification in this audit, no specific control is attributed to it.[20, 21, 22, 23]

3. Literature, Gap and Novelty

Technical guidance recommends lifecycle controls: preserve originals, document provenance and transfers, restrict access, record transformations and repeat integrity checks. NISTIR 8387 and NIST's 2025 summary of a U.S. evidence-handlers survey support written standards, audits and performance indicators. These materials are comparators, not evidence about Bilaspur.[24, 25]

Indian legal scholarship after the BSA has examined the move from the former Section 65B framework, the certificate's scope, hash values, expert participation and trial-level procedural difficulties. M. Suhail Salafi's October 2026 article in this journal is particularly relevant. It discusses trial-court challenges involving certificates, metadata and source systems, and advocates case-management and forensic standardisation. It would be inaccurate to claim that earlier work has not addressed practical Section 63 problems. This paper asks a narrower

[20] e-Committee, Supreme Court of India, Digital Preservation—Standard Operating Procedure (Version 1.2, Nov. 29, 2022), https://thc.nic.in/user%20manual/Digital%20Preservation%20SOP.pdf.
[21] e-Committee, Supreme Court of India, Digital Preservation—Standard Operating Procedure (Version 1.2, Nov. 29, 2022) (preservation metadata, access controls, timestamped digitisation logs and transfer tracking). The SOP predates the BSA and addresses preservation, not a complete live-evidence intake procedure under § 63.
[22] Jitendra Kumar Rode v. Union of India, SLP (Crl.) No. 2063/2023, order at 2–3 (India Apr. 24, 2023), https://api.sci.gov.in/supremecourt/2023/5292/5292_2023_8_1504_43930_Order_24-Apr-2023.pdf.
[23] High Court of Chhattisgarh, SOP No. 9698/CPC/2025, SOP for Digital Preservation of Records of the Chhattisgarh High Court and District Courts (May 27, 2025), listed in the High Court's official rules/SOP index. The publicly accessible index confirms the instrument's title and date; this audit does not attribute unverified operational clauses to it.
[24] Nat'l Inst. of Standards & Tech., Digital Evidence Preservation: Considerations for Evidence Handlers (NISTIR 8387, 2022), https://doi.org/10.6028/NIST.IR.8387.
[25] Nat'l Inst. of Standards & Tech., New Report Reveals Evidence Handlers' Common Practices, Makes Recommendations (Dec. 2025), https://www.nist.gov/news-events/news/2025/12/new-report-reveals-evidence-handlers-common-practices-makes-recommendations (summarizing a U.S. national evidence-handlers survey).

question: what do public documents and institutional reports show about Bilaspur's administrative readiness, and do their published interfaces form one auditable evidence lifecycle? The analysis concerns documentary design, not actual compliance rates.[26]

The paper's contribution is a local systems crosswalk and an implementation model. It reads the BSA Schedule alongside the 2020 e-filing hash rule, the 2025 eSakshya event-packet rules, court-preservation guidance, the reported Bilaspur paperless court/e-Malkhana launch and the transition issue raised by a local interim order. The distinction among acquisition, registry receipt and court archive matters operationally. The same digest may recur when the bytes remain unchanged, but each checkpoint has a different custodian, time, purpose and audit event. A hash verifies byte identity against a recorded value. It cannot fill a gap in custody documentation or establish that a record is complete.[27, 28, 29, 30]

4. Objectives, Questions and Hypotheses

The study has four objectives: (1) identify the statutory and transitional rules governing proof of electronic records after the BSA commenced; (2) map the publicly documented police, filing, courtroom and preservation arrangements relevant to Bilaspur; (3) identify administrative risks for investigating officers, advocates, registry staff and judicial officers without attributing unobserved errors to them; and (4) design a court-led SOP and evaluation framework that connects technical integrity controls with Section 63 certificates.

The study asks three questions: (a) What do public legal and administrative materials specify about acquisition, certification, filing, access and preservation? (b) Where do local instruments describe related controls but leave their interoperability unspecified? (c) What minimum SOP would make an item's identity and custody auditable while leaving admissibility to the court?

H1 (documentary-readiness hypothesis): Bilaspur's publicly documented position is better characterised as an integration and certificate-interface challenge than as an absence of foundational digitisation. Formal eSakshya, e-filing and preservation arrangements coexist, but their published instruments do not describe a common item-level Section 63 lifecycle. The audit assesses H1 against the document corpus. Any support for H1 concerns public documentation,

[26] See supra note 7.
[27] See supra note 14.
[28] See supra note 21.
[29] See supra note 12.
[30] See supra note 3.

not actual system performance. H2 (implementation hypothesis): A common item-level protocol linking identifiers, acquisition/receipt/archive integrity events, both certificate parts, access logs and retention should reduce avoidable administrative defects while preserving judicial discretion. H2 is a testable design proposition; this audit cannot establish a causal reduction without prospective operational data.

5. Methodology and Scope

This bounded documentary audit purposively selected primary legal and institutional materials available through 31 October 2026: the BSA; Chhattisgarh's e-filing rules and 2025 eSakshya Rules; national and state preservation instruments; relevant Supreme Court and Chhattisgarh High Court decisions; official e-Committee reports on Chhattisgarh and Bilaspur; and comparative technical literature. Close reading begins on 1 July 2024, with earlier rules serving as baselines. Sources were chosen for their relevance to creation, certification, transfer, court access, preservation, appeal or privacy.

The audit coded sources against eight controls: provenance; acquisition hash/certificate; registry validation; cross-system identifiers; custody/access logs; court access/disclosure; retention/appeal; and privacy/exceptions. Each finding is labelled "explicit," "partly specified," or "not publicly specified in reviewed instruments." The last label describes the public record; it does not establish that a control is absent in practice. No composite score is used because non-publication does not prove non-implementation.

The study is empirical in the limited sense that it compares published rules and institutional outputs against defined lifecycle controls. It is not a field survey. No stakeholder interviews, Bilaspur case-file sample or system logs were available. Here, "bottlenecks" means structural friction implied by the rules, not measured prevalence or reported user experience. One interim local order illustrates transition complexity but is not representative. These limits govern the conclusions.

6. Documentary Findings

The documents support H1 to a limited extent. They show a statutory certificate design, a state police evidence-packet and routing framework, an e-filing hash requirement for online audio/video, national preservation guidance, and the reported launch of a paperless court and e-Malkhana in Bilaspur. The main gap in the reviewed materials is not a demonstrated lack of

technology. It is the absence of a publicly documented, end-to-end crosswalk that reconciles each tendered item's identity, certificates, integrity events, logs and retention across these systems. The matrix records what the instruments specify.

Lifecycle control	**What the public record specifies**	**Readiness finding in this audit**
BSA proof	Section 63(4) and its Schedule prescribe particulars, hash details and Part A/Part B certification.	The legal baseline is explicit. The statute does not set out court-side verification or a cure process.
Police capture	The 2025 eSakshya Rules prescribe a secure packet, SID, timestamps, geolocation, hash, immutable storage and an e-signed Part A certificate.	Controls are detailed for covered events and records. Broader sources and the Part B interface need operational mapping.
Registry receipt	Published e-filing Rule 8.4 requires the Administrator to hash online audio/video filings.	A filing checkpoint is specified. The text does not explain how it relates to the acquisition hash or certificate.
System identifiers	eSakshya links the SID to FIR/general-diary data and describes court access through CIS/Sakshya Portal on ICJS.	Police-to-court routing is described at a high level. The reviewed public materials do not identify a SID-to-CNR/e-filing crosswalk.
Logs and custody	National preservation guidance covers access controls, timestamped digitisation logs and transfer tracking.	These controls appear across preservation guidance. The reviewed instruments do not publicly specify one live-evidence exception and access-log record.
Archive and appeal	eSakshya provides an archival mode after trial; e-filing Rule 10.2 addresses retention through final disposal, including superior appeal.	Retention is addressed across instruments, but the reviewed documents do not provide one retention-trigger and disposition matrix for all digital evidence.
Privacy and	The eSakshya and e-filing rules	The legal basis is present. The SOP

Lifecycle control	What the public record specifies	Readiness finding in this audit
access	address court access and sharing, as well as confidentiality or privacy exceptions.	should log roles, purposes, redactions, exports and reviews.

The matrix is not a compliance rating. Bilaspur's reported e-Malkhana indicates a case-property management initiative and a move towards paperless processes. It does not establish that the system stores every electronic record, independently validates hashes or produces a BSA Part B certificate. The eSakshya Rules provide acquisition metadata for covered events, but they do not show that every record later tendered in court passed through the app. Readiness depends on how these systems connect as well as on their existence.[31, 32]

7. Administrative Friction Points

For investigating officers, the main risk is a weak hand-off between field capture and the case record. eSakshya covers specified events, but electronic material may also come from CCTV operators, service providers, personal devices, cloud accounts or other third parties. The person signing Part A may differ from the officer who receives the file, and an examiner may later certify a derivative. Without an item ID, acquisition method, time zone, hash algorithm and custody receipt, a valid hash of a copy may not show how it relates to the source. This is a design risk, not a finding about Bilaspur officers' conduct.

For advocates and prosecutors, Section 63(4)'s phrase "each instance" makes filing preparation and transition screening essential. A checklist should record the commencement date, source, Part A signatory, Part B expert, hash report and any transformations. Counsel should not certify facts outside their knowledge of the originating system. A judicial direction to complete or correct a certificate should specify the required route and time. Vineet Fules illustrates a local dispute over a late certificate, but establishes no general rule on curing defects.[33, 34, 35]

[31] See supra note 18.
[32] See supra note 3.
[33] See supra note 4.
[34] See supra note 11.
[35] See supra note 12.

For the registry, intake validation and admissibility are separate functions. Rule 8.4 creates a hash checkpoint for online audio/video filings. Staff should identify the submitted object, record its receipt hash without changing it, issue a receipt and refer mismatches for judicial direction. Registry staff should not decide relevance or authenticity. If eSakshya and registry hashes differ after compression, segmentation or export, an exception record should describe the transformation and preserve both objects where lawful. The reviewed rules do not specify a public reconciliation form.[36, 37]

Unresolved identifiers can increase search and disclosure costs. An SID, FIR/general-diary number, CNR, e-filing ID, malkhana number and archive accession may all relate to the same item. Staff need reliable access to the source, certificate, hash report and event log; judges retain authority over proof, objections and remedies. Preservation access controls and transfer tracking provide a useful base, but they should connect to the live-evidence history.[38, 39]

Record access must be controlled while preserving fair disclosure. Electronic evidence may contain personal data, location traces, confidential third-party material or sensitive information about victims. The record should show who viewed or downloaded an item, why access was granted, whether a redacted copy was made and which version was supplied to the accused or another entitled party. Privacy should not become an unreviewed reason to withhold material needed for a fair hearing. Courts should be able to review and document access restrictions and redactions. These safeguards arise from the interaction of local confidentiality rules, disclosure duties and constitutional privacy principles.[40, 41, 42]

8. Proposed Bilaspur SOP for Section 63 Evidence Management

The High Court, working with the State Home Department, police, prosecution, forensic services and district judiciary, should adopt an evidence-intake addendum linking the BSA with eSakshya, e-filing and digital-preservation systems. Before adoption, it should confirm the current consolidated text of the 2020 e-filing rules and the operative clauses of SOP No.

[36] See supra note 5.
[37] See supra note 14.
[38] See supra note 20.
[39] See supra note 21.
[40] See supra note 15.
[41] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[42] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; Chhattisgarh eSakshya Management Rules, 2025, r. 8; High Court of Chhattisgarh, Rules for Online Electronic Filing, Notification No. 6102/Rules/2020, r. 12.

9698/CPC/2025. The protocol below is an administrative control. It creates no new admissibility condition and does not limit judicial discretion.[43, 44]

8.1 One item record and three integrity checkpoints

For a source outside eSakshya, assign that ID at first authorised acquisition or receipt.

The item record should distinguish three checkpoints. At acquisition, record the source, collector or receiving custodian, date and time with time zone, relevant location, method or tool, device or service details, native filename and format, hash algorithm and value, and known limitations. At registry receipt, record the submitting party, receipt time, object name, size and format, receipt hash, certificate status, and whether the submitted bytes match the acquisition object or form a documented derivative. At archival deposit, record the destination, responsible official, archive hash or revalidation result, storage class, retention trigger and any migration. If the bytes are unchanged, the same digest may appear at all three checkpoints, but each event must have its own log entry. SHA-256 should be the default unless a legally approved standard changes. Retain legacy or source-system values as recorded; do not overwrite them. The BSA Schedule and applicable law remain controlling.[45, 46]

8.2 Certificate and source-object workflow

The originating or responsible person should complete the applicable Part A information. Where the eSakshya Rules apply, use the certificate generated by the app. Part A must accompany the exact object or a clearly identified derivative. An expert completing Part B should record the examination, tools and versions, hash inputs, limitations and conclusion required by the Schedule. An SOP should not define expert qualifications beyond the law; the court must resolve disputed qualifications. If Part B is not yet available, registry staff should mark the certificate incomplete and place the matter before the court under the applicable procedure. They should neither reject it summarily nor treat the record as proved.[47, 48, 49]

---

[43] See supra note 23.
[44] See supra note 16.
[45] See supra note 4.
[46] High Court of Chhattisgarh, Rules for Online Electronic Filing, Notification No. 6102/Rules/2020, rr. 8.4, 10.2 (July 10, 2020); e-Committee, Supreme Court of India, Digital Preservation—Standard Operating Procedure (Version 1.2, Nov. 29, 2022).
[47] See supra note 9.
[48] See supra note 18.
[49] See supra note 10.

Preserve the original as read-only where feasible. Conduct analysis, redaction, transcoding, playback conversion and export on a working copy. Give each derivative a linked item relationship, hash, creation event, tool and version, operator, reason and parent-object identifier. A manifest should list every file in the packet and its hash, including certificates and expert reports. The manifest does not replace the statutory certificate. If a device clock differs from trusted time, record the discrepancy and how any estimate was made; do not silently normalise it.

8.3 Registry receipt, exceptions and court use

At e-filing, the registry should run a non-destructive integrity and readability check, confirm that the file opens with an approved tool, preserve the submitted bytes and record the receipt hash. For audio/video, this implements Rule 8.4. The SOP may extend the same administrative check to other electronic records. The registry checklist should confirm an Evidence Item ID, relevant source identifier, file manifest, Part A and Part B status, hash report, and retention or privacy flag. Staff should refer mismatches, missing certificate fields, damaged files, unsupported formats and identifier conflicts to a registrar-designated technical officer, then place legally material disputes before the judge promptly. Registry staff should not decide admissibility, authenticity or evidentiary weight.[50, 51]

For hearings and disclosure, the court should use a verified working copy linked to the preserved original. The system should log access, export, playback and redaction events, including the actor, role, date and time, purpose, item and version, action, and outcome. As the court directs, parties should receive an accessible copy or supervised access, with a recorded hash and disclosure receipt. Mark each redacted or converted version as a derivative and link it to its unredacted parent under appropriate restrictions. The bench should be able to retrieve the certificate, source metadata, custody log and expert explanation without depending on one portal or local storage path.

8.4 Retention, migration, privacy and continuity

Where the system permits, move an archival copy into preservation mode after trial. Archive mode must not delete the item or sever it from the case record. Tie retention to final disposal, including any applicable superior appellate process, and to judicial preservation orders, appeals, retrials or collateral proceedings. The retention schedule should distinguish working copies,

[50] See supra note 14.
[51] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(4); Pune Bar Ass'n, 2026 SCC OnLine SC 1297.

source objects, certificates, manifests, access logs and audit exports. Before migration or format conversion, verify and record the original hash, tool, destination and hash of the new derivative. Retain source bytes when practicable and legally permitted. Quarterly restoration checks should confirm that preserved items can be retrieved and verified.[52, 53, 54]

Use role-based access and the principle of least privilege. Every search, view, copy, export, share, redaction and deletion attempt should create a tamper-evident audit event. Assign a named custodian to sensitive records and record the court-approved basis for access or redaction, with a review or expiry date for restrictions. Separate backups from routine user credentials, test them, and protect data in transit and at rest. Published Rule 8.7 prohibits encryption of online e-file documents; its wording and current consolidated status must be confirmed. The protocol must follow the operative rule. Court administration should distinguish that provision from safeguards for transmission, storage and backups, and formally approve any encryption method that could conflict with current rules.[55, 56, 57]

8.5 Offline exceptions, governance and performance review

Evidence captured during a network outage, emergency or application failure should remain part of the record. The officer should preserve the original on approved media, complete a numbered offline event form, record the source and custody, calculate a hash when an approved tool becomes available, and upload the packet with an exception code and reason. Preserve both the event time and upload time. A supervisor should review unresolved exceptions within a set period. At filing, the SOP should screen matters instituted before commencement under Section 170(2) and seek judicial direction where the governing evidentiary regime is disputed.[58, 59]

A joint High Court–Home Department implementation group should maintain the data schema, approved hash and tool list, role matrix, exception codes, training materials and version history. Begin with a 90-day Bilaspur pilot, using a prospectively defined baseline and including

[52] See supra note 15.
[53] Chhattisgarh eSakshya Management Rules, 2025, Notification No. ESTB/1255/2025-Home Section, rr. 2(g), 4–7, 9, 11 (Apr. 19, 2025); High Court of Chhattisgarh, Rules for Online Electronic Filing, Notification No. 6102/Rules/2020, rr. 8.4, 10.2, 12 (July 10, 2020).
[54] e-Committee, Supreme Court of India, Digital Preservation—Standard Operating Procedure (Version 1.2, Nov. 29, 2022); High Court of Chhattisgarh, SOP No. 9698/CPC/2025, SOP for Digital Preservation of Records of the Chhattisgarh High Court and District Courts (May 27, 2025).
[55] See supra note 14.
[56] See supra note 15.
[57] See supra note 42.
[58] See supra note 11.
[59] See supra note 6.

police-originated, third-party and advocate-filed electronic records. Without ranking individual staff, report: (1) first-submission completeness of item identifiers and certificate fields; (2) hash mismatch and resolution rates; (3) time to cure missing or inconsistent paperwork; (4) the share of transfers with complete access and custody logs; (5) time to provide court-directed party access; (6) retrieval and restoration success; and (7) privacy incidents and exception frequency by source type. Publish aggregate results, review failures and revise the SOP before expansion. These are proposed indicators, not measurements of current Bilaspur performance.[60, 61]

9. Discussion and Limitations

The documentary evidence supports H1: Chhattisgarh has substantial digitisation and evidence-management components, but the public instruments reviewed do not show a shared record that reconciles item identifiers, certificate parts, integrity events, custody and access logs, and appellate retention. This finding concerns public documents; it does not prove that system integrations or internal protocols are absent. The reported paperless court and e-Malkhana are positive readiness signals. A process audit should test interoperability and documentation before drawing conclusions about equipment.[62, 63, 64]

H2 remains untested. The proposed protocol is intended to reduce ambiguity and rework by assigning an owner, identifier and record to each event. A pilot must assess it under local staffing, training, network and portal conditions. Its indicators should measure process rather than judicial conclusions. The Supreme Court's 2026 ruling confirms the statutory importance of hash and expert certification, but it prescribes no local workflow.[65, 66]

The study has three limitations. It does not examine Bilaspur case files or system telemetry. It could not verify the substantive text of the listed 2021 e-filing amendment or the 2025 records-preservation SOP, and it had no interview or survey data. The audit therefore identifies structural risks, not their frequency, cause or effect on users. Follow-up research should sample filings, code certificate and hash completeness, interview advocates, registry officials, police and experts, and compare indicators before and after an SOP pilot under privacy safeguards.

---

[60] See supra note 25.
[61] Nat'l Inst. of Standards & Tech., Digital Evidence Preservation: Considerations for Evidence Handlers, NISTIR 8387, at 3–8 (2022) (integrity, provenance, transfer records and access controls).
[62] See supra note 2.
[63] See supra note 3.
[64] See supra note 23.
[65] See supra note 10.
[66] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63; Pune Bar Ass'n, 2026 SCC OnLine SC 1297.

10. Conclusion

Section 63's certificate and hash requirements make digital evidence management a chain of accountable events. Bilaspur's public record shows a strong foundation: eSakshya packets and Part A, e-filing hashes for online audio/video, national preservation guidance, a listed local preservation SOP, and the reported paperless court and e-Malkhana. These components appear in separate instruments; the reviewed public materials do not show a single Section 63 workflow. That supports H1's integration focus but does not establish non-compliance.

The SOP creates one Evidence Item ID, logs acquisition, registry and archive integrity events separately, links certificates to each source or derivative, preserves custody and access logs, and retains records through appeal. It keeps admissibility with judges and makes access and privacy decisions auditable. Adoption should follow verification of current rules and a supervised pilot; Bilaspur's performance remains unmeasured.