

Standards

www.qualitymag.com/articles/99714-why-inspection-bodies-should-think-differently-about-digital-evidence-under-iso-iec-17020-2026

Image credit: Halfpoint / iStock / Getty Images Plus (Creative #1087179422)

Why Inspection Bodies Should Think Differently About Digital Evidence Under ISO/IEC 17020:2026

The transition period runs until March 27, 2029, with accreditation bodies beginning assessments from September 2026.

[Nemat Baghernejad](#)

July 2, 2026

When ISO/IEC 17020:2026 was published on March 27, 2026, it landed quietly in most inboxes. The title was familiar. The structure was recognizable. But inside were clauses that represent a fundamental shift in how inspection bodies must govern their digital information — and the implications are more significant than many quality leaders have yet recognized.

The 2012 edition acknowledged electronic records. The 2026 edition regulates them. That distinction matters.

What the New Standard Actually Requires

Data and information control is now a standalone requirement with no equivalent in the 2012 edition. Inspection bodies must implement documented procedures that address [software validation](#), data integrity assurance, protection against unauthorized access, and system failure logging. Data cannot be tampered with without detection, and breaches must be addressed through corrective action.

Technology systems, [AI tools](#), and remote inspection platforms now require formal validation records and change management procedures. Using a digital tool without formal validation documentation constitutes a nonconformity.

Externally provided services now include IT providers. Inspection bodies must maintain a mandatory provider register covering any external service that affects inspection results.

Inspection record integrity expectations are significantly stronger. Reports must be traceable to the specific inspector, method, equipment, and date — with demonstrable evidence that the record has not been altered after issuance.

The transition period runs until March 27, 2029, with accreditation bodies beginning assessments from September 2026 — a window narrower than it appears.

The Problem Conventional Tools Cannot Solve

Inspection bodies will respond logically: review document management platforms, tighten access controls, add software validation records. That satisfies the basic intent of the new requirements. But there is a specific problem conventional tools — SharePoint, inspection software, custom [ERP](#) — cannot address regardless of

configuration. It is the multi-party trust problem.

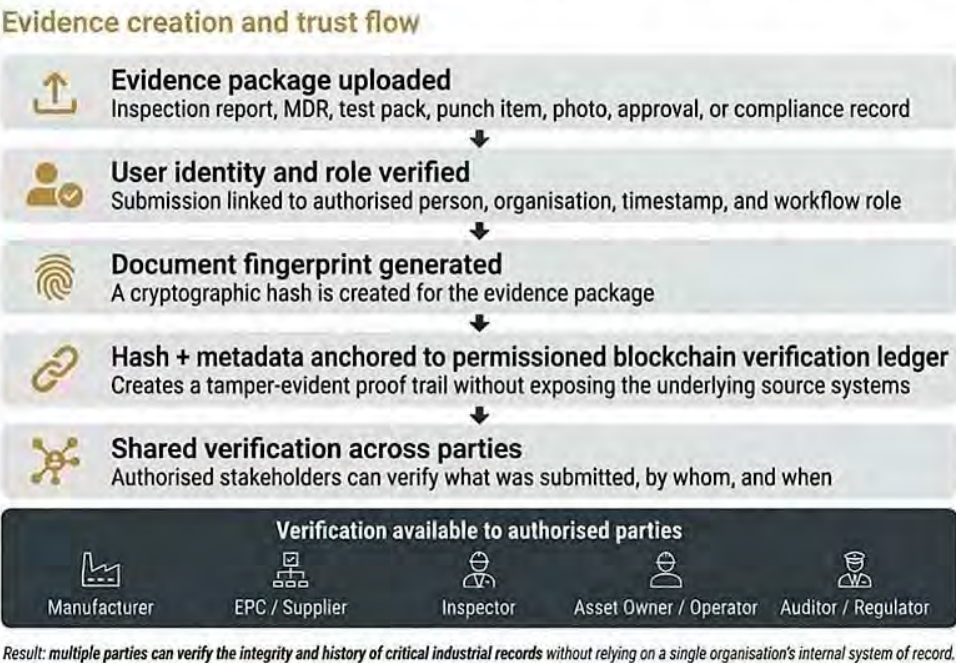
Consider a typical source inspection: a third-party body inspects equipment made by Party A, on behalf of asset owner Party B, with subcontractors from Party C, and auditor Party D reviews the results. Each party holds its own copy of the record. When a warranty dispute arises eighteen months later, versions differ, and there is no mechanism to determine which is authentic.

The reason is structural. Conventional systems are single-party: the controlling organization manages access, maintains logs, and can — theoretically — alter, delete, or backdate records. This creates “self-attested” evidence. A global admin can manipulate version history. A database admin can edit audit logs. A digital signature proves who signed, not that the document is unchanged since signing. In warranty disputes, regulatory audits, and arbitration, self-attested evidence is vulnerable to challenge.

How Permissioned Blockchain Addresses the Gap

As shown in Figure 1, each inspection evidence package moves through a simple flow: upload, identity and role verification, cryptographic fingerprinting, anchoring to a permissioned blockchain verification ledger, and verification made available to authorized parties across the supply chain.

Figure 1 — How ALMFlux creates a shared, tamper-evident evidence trail



Source: Nemat Baghernejad

Figure 1 — How permissioned blockchain creates a shared, tamper-evident evidence trail

A permissioned blockchain creates a shared, immutable ledger in which no single party controls the historical record. Each inspection document is cryptographically hashed using SHA-256 at the moment of submission. That hash, with the submitting party’s verified identity and timestamp, is anchored to the distributed ledger. Any modification — changing a single character — produces a completely different hash, immediately detectable by any authorized party.

The result is “independently verifiable” evidence: authenticity is confirmed by comparing the document’s current hash against the ledger — no access to the inspection body’s internal systems required, and no administrative action can defeat it.

Figure 2 shows the same logic in a cleaner technical sequence: inspector uploads report, identity is verified through role-based credentials, a SHA-256 hash is computed, the hash is anchored to a Hyperledger Fabric ledger, and multi-party verification access is then provided to stakeholders including the manufacturer, inspector, supplier, asset owner, and auditor.



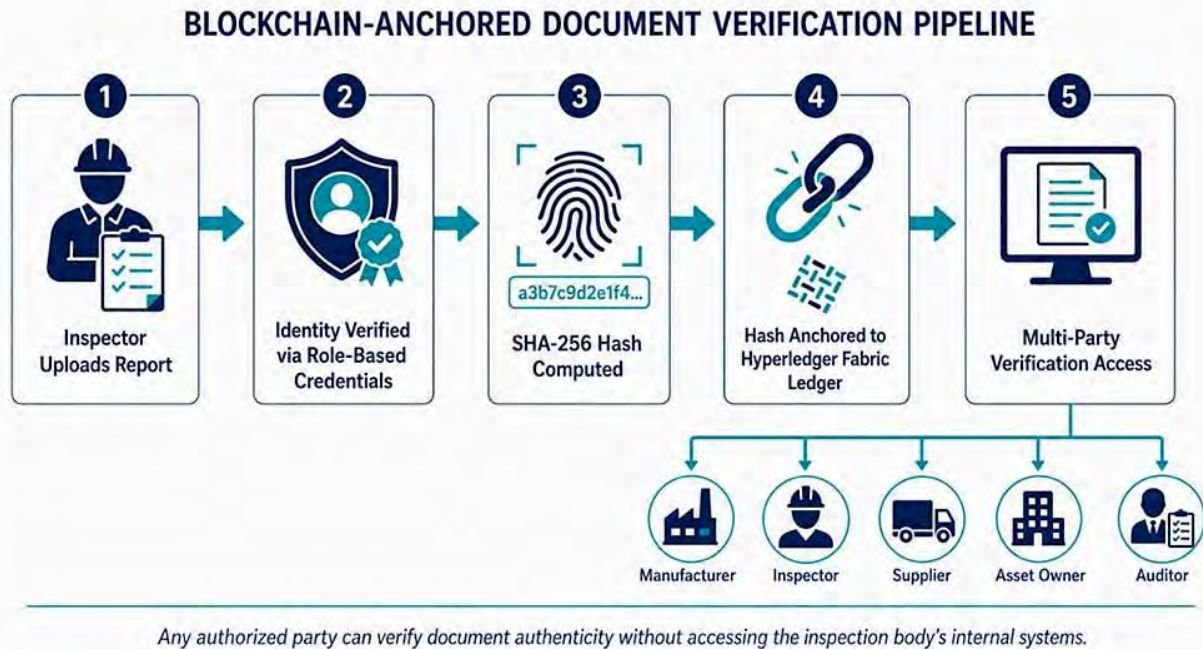


Figure 2 — Blockchain-anchored document verification pipeline

Source: Nemat Baghernejad

Figure 2 — Blockchain-anchored document verification pipeline

Hyperledger Fabric, maintained by the Linux Foundation, is well-suited to inspection operations: identity-verified participants, channel-based data privacy, energy-efficient consensus, and programmable smart contract logic to enforce workflow rules.

The Evidence Quality Distinction

The fundamental differentiator is not functionality — both conventional tools and blockchain can store documents, manage versions, and control access. The difference is the nature of the evidence produced.

- Warranty disputes. Self-attested evidence requires proving a negative — that systems were never altered. Independently verifiable evidence inverts this: any party confirms the hash matches, mathematically, without relying on anyone's attestation.
- Accreditation audits. Assessors under 17020:2026 look not just for procedures, but for evidence those procedures work. Blockchain provides a structural demonstration of tamper-evident record management.
- Commercial tenders. GCC asset owners increasingly specify digital verification in TPI tender criteria.

The inspection body that offers “verify it yourself” wins contracts; the one that offers “trust us” cannot.

What a Practical Pilot Looks Like

The business case does not require an organization-wide transformation. A scoped pilot — two to three live projects within a single regional office, running parallel to existing processes over 12 weeks — provides sufficient data for an evidence-based go/no-go decision.

Target metrics: 70%+ reduction in documentation processing time; audit-ready compliance packages within one business day (versus weeks currently); near-zero unresolved record discrepancies; stakeholder satisfaction of 4/5 or above.

One important clarification: blockchain complements, not replaces, a functioning quality management system. The standard does not mandate any specific technology. The case for blockchain is about evidence quality and the competitive and legal advantages independently verifiable records create — not compliance sufficiency alone.

Looking Beyond 2029

The EU's Ecodesign for Sustainable Products Regulation, with delegated acts expected from 2027, will require Digital Product Passports mandating cradle-to-grave traceability of product data, including inspection records. Blockchain-anchored records are inherently compatible with this framework, giving inspection bodies compounding value: 17020:2026 compliance readiness, commercial differentiation, dispute resilience, and regulatory future-proofing in a single architecture.

The March 2029 deadline allows time for thoughtful adoption. But September 2026 — when accreditation bodies begin formal transition assessments — is closer than it looks.



- **Governing Artificial Intelligence in Conformity Assessment: The ISO/CASCO Perspective**
- **Manufacturers Must Unify Data Now to Meet First Digital Product Passport Deadlines**
- **From QSR to QMSR: What Medical Device Manufacturers Need to Change—and What They Don't**



Nemat Baghernejad is a CSWIP 3.2, Senior Industrial Inspector with over a decade of source inspection experience across GCC oil and gas projects and 30+ industry qualifications including ASNT Level II. He is Founder of ALMFlux Technologies Ltd (DIFC, Dubai). For more information, visit contact@almflux.com.

Disclosure: The author is the Founder of ALMFlux Technologies Ltd, which develops blockchain infrastructure for the inspection industry.

