How Verifiable Time Supports Regulatory Compliance

Strengthening Auditability, Traceability and Trust in Digital Records

> **A timestamp records that something happened. Verifiable time provides evidence of when it happened, in what sequence, and whether the record can still be trusted.**

Regulatory compliance increasingly depends on an organization's ability to demonstrate what happened, when it happened and in what sequence events occurred.

Financial transactions are executed in fractions of a second. AI agents make or influence decisions without continuous human supervision. Automated machines respond to changing conditions in real time. As these systems generate growing volumes of timestamps, logs and audit records, regulatory frameworks increasingly emphasize transparency, traceability and accountability.

Yet the existence of a timestamp does not prove that the time was accurate, that the record has remained unchanged or that timestamped events occurred in the sequence reported. As digital records move among organizations operating on different platforms or in different jurisdictions, establishing a common and defensible chronology becomes more difficult.

Important questions can arise:

- Was the system clock accurate when the record was created?
- Could the timestamp or underlying record have been changed afterward?
- Did one event occur before or after another?
- Was the record created contemporaneously or reconstructed later?
- Do separate systems provide a consistent account of the same activity?
- Can an outside party verify the chronology without relying entirely on the organization that produced it?

Verifiable time helps address this evidentiary gap. By linking digital events to an independently examinable, tamper-evident time reference, it makes possible a durable record that can be compared against a shared chronology rather than accepted solely as the assertion of an individual system.

Verifiable time does not replace the policies, controls, documentation or professional judgment required for compliance. It can, however, strengthen the evidence organizations use to demonstrate that required processes were followed and that the resulting records are credible.

FROM RECORDKEEPING TO PROOF

Many regulations require organizations to maintain records of transactions, decisions, system changes, data processing and security incidents. Depending on the applicable requirements, those records may need to be accurate, complete, traceable, securely retained and available for examination.

Organizations generally address these obligations through internally generated logs and database timestamps. Those records may be reliable for day-to-day operations, but their evidentiary value can become less certain when they are shared with customers, counterparties, auditors or regulators—or when records from several systems must be reconciled.

The distinction is between recording a time and being able to verify it. A synchronized system clock helps establish an accurate timestamp. Verifiable time adds evidence that can help show when the timestamp was established, where the associated event belongs in a sequence and whether that chronology has remained intact.

This additional layer can be especially valuable when an audit, dispute or investigation occurs months or years after the underlying event.

SUPPORTING CORE COMPLIANCE FUNCTIONS

Although regulations vary by industry and jurisdiction, many contain requirements involving auditability, traceability, record integrity or the reconstruction of events. Verifiable time can support these functions in several ways.

Audit Trails and Record Integrity

An audit trail should show not only the current state of a record, but also how and when that record was created, accessed or changed. Verifiable time can strengthen an audit trail by providing independent evidence of the timing and sequence of recorded actions. It can also make retrospective changes to an established chronology more readily detectable.

Traceability

Traceability requires organizations to reconstruct the history of an action, transaction or decision. This may involve following information across several systems and establishing which inputs, approvals and changes preceded an outcome. A shared time reference can help connect records produced by otherwise independent systems. This is particularly valuable when no single organization controls the entire process.

Accountability for Automated Decisions

When an AI system, smart contract or autonomous machine initiates an action, reviewers may need to determine what the system did, which information was available and what rules or model version governed the decision. Verifiable time can help establish when each relevant input, decision and response was recorded, improving the ability to reconstruct an automated process after the fact and attribute actions to the conditions under which they occurred.

Incident Investigation and Reporting

Cybersecurity, privacy and operational-resilience requirements often require organizations to identify incidents, assess their effects and report them within specified periods. Accurate chronology is essential to determining when an incident began, when it was detected, which systems were affected and when corrective action was taken. Verifiable records can support this reconstruction and provide stronger evidence that reports were based on contemporaneous information.

Regulatory Reporting and Dispute Resolution

Regulators may compare records from multiple market participants, service providers or operational systems. If the underlying timestamps are inconsistent or cannot be independently examined, reconstructing events can become difficult. A common, verifiable time reference can provide an additional evidentiary layer for resolving discrepancies and demonstrating the sequence in which events took place.

CLOCKCHAIN AS A COMPLIANCE EVIDENCE LAYER

Clockchain is designed to create a continuously recorded and independently verifiable chronology. It aggregates multiple independent, trusted time sources to establish a unified reference aligned with Coordinated Universal Time. That reference is validated through network consensus and recorded on-chain every second.

Applications and organizations can use this chronology to create verifiable proof associated with digital events. Depending on the implementation, this may help demonstrate:

- when a transaction, decision or system action was recorded;
- the order in which related events occurred;
- that a particular record existed at a particular point in time;
- whether the chronology of logged events has remained consistent;
- whether separate systems agree about the timing of shared activity; and
- whether compliance evidence was created contemporaneously rather than reconstructed later.

Clockchain is not a substitute for legal advice, regulatory interpretation or a complete compliance program. It does not determine whether an organization has met every substantive or procedural requirement of a particular law. Nor does it replace required synchronization systems, access controls, cybersecurity safeguards, validated applications or retention policies.

Implementation must also account for privacy, confidentiality and data-governance requirements. Sensitive or personal information need not be placed directly on-chain; cryptographic proofs can be used to verify records while the underlying data remains within appropriately controlled systems.

Clockchain strengthens the integrity and credibility of the evidence on which regulatory compliance depends.

BUILDING A MORE DEFENSIBLE RECORD

Regulators do not generally require organizations to use blockchain technology or any particular verifiable-time network. They do, however, increasingly expect organizations to maintain reliable records, reconstruct digital activity and demonstrate that required controls operated as intended.

As transactions become faster, systems become more autonomous and digital processes extend across organizational boundaries, internally generated timestamps may provide an incomplete basis for trust. Verifiable time adds an independent layer of evidence, helping transform a timestamp from a system's assertion into part of a durable and examinable chronology.

Existing compliance systems document what an organization says happened. Verifiable time can provide stronger proof of when it happened and the sequence in which events took place.

The accompanying appendix identifies regulations, standards and frameworks from around the world for which accurate time, reliable logs, event sequencing or tamper-evident records may be relevant. Applicability and implementation requirements will vary by organization, industry and jurisdiction.

Appendix: Global Regulations, Standards and Frameworks Relevant to Verifiable Time

Current as of August 2026

PURPOSE AND SCOPE

This appendix identifies selected laws, regulations, technical standards and supervisory frameworks for which accurate time, reliable timestamps, synchronized clocks, tamper-evident logs or defensible event chronology may be relevant.

Some requirements expressly mandate synchronized clocks or time-stamped audit trails. Others require organizations to retain reliable records, reconstruct automated decisions, document security incidents or demonstrate when regulatory obligations were performed.

Verifiable time does not, by itself, establish compliance with any of these requirements. It can provide an additional evidentiary layer that helps organizations demonstrate when events occurred, how those events were sequenced and whether the resulting chronology has remained intact.

RELEVANCE CLASSIFICATIONS

- **Direct:** The requirement expressly addresses timestamps, clock synchronization or time-stamped audit trails.
- **Strong:** The requirement involves logging, event reconstruction, incident reporting or record integrity for which reliable chronology is important.

ARTIFICIAL INTELLIGENCE AND AUTOMATED DECISION-MAKING

1. EU Artificial Intelligence Act

Jurisdiction: *European Union* **|** ***Relevance:*** *Strong*

Article 12 requires high-risk AI systems to support automatic event logging for traceability. Articles 19 and 26 establish related log-retention obligations for providers and deployers. Verifiable time can strengthen the chronology of system inputs, decisions, interventions and outputs.

Official source: Regulation (EU) 2024/1689—Artificial Intelligence Act

FINANCIAL MARKETS, BANKING AND DIGITAL ASSETS

2. MiFID II and MiFIR Business-Clock Requirements

Jurisdiction: *European Union* **|** ***Relevance:*** *Direct*

The MiFID II/MiFIR framework requires trading venues, market participants and specified reporting entities to synchronize the business clocks used to record reportable events. Current technical standards establish Coordinated Universal Time as the reference and prescribe accuracy and maximum-divergence requirements for different types of trading activity.

Official source: Commission Delegated Regulation (EU) 2025/1155

3. SEC Rule 613 and the Consolidated Audit Trail

Jurisdiction: *United States* **|** ***Relevance:*** *Direct*

SEC Rule 613 requires national securities exchanges, FINRA and their members to synchronize the business clocks used to record reportable events. Timestamps reported to the Consolidated Audit Trail generally must use millisecond or finer increments, subject to provisions applicable to particular events.

Official source: U.S. Securities and Exchange Commission—Rule 613

4. SEC Rules 17a-3 and 17a-4

Jurisdiction: *United States* **|** ***Relevance:*** *Direct*

SEC broker-dealer recordkeeping rules require specified records to be created and preserved for defined periods. Permitted electronic preservation methods include a complete, time-stamped audit trail showing record modifications and deletions, the date and time of actions and, where applicable, the identity of the person responsible.

Official source: 17 CFR § 240.17a-4

5. Digital Operational Resilience Act

Jurisdiction: *European Union* **|** ***Relevance:*** *Strong*

The Digital Operational Resilience Act, or DORA, requires covered financial entities to detect, manage, record and report information and communications technology incidents. Article 17 specifically requires organizations to identify, track, log, categorize and classify such incidents.

Official source: Regulation (EU) 2022/2554—DORA

6. Markets in Crypto-Assets Regulation

Jurisdiction: *European Union* **|** ***Relevance:*** *Strong*

The Markets in Crypto-Assets Regulation, or MiCA, establishes recordkeeping and supervisory requirements for crypto-asset service providers. Supporting technical standards require providers to preserve specified information concerning client orders and transactions.

Official source: Commission Delegated Regulation (EU) 2025/1140—MiCA Recordkeeping Standards

7. UK Financial Conduct Authority Recordkeeping and Clock Rules

Jurisdiction: *United Kingdom* **|** ***Relevance:*** *Direct*

The FCA Handbook contains record-retention requirements for regulated firms and clock-synchronization requirements for specified trading activities. Relevant firms must retain records sufficient to demonstrate compliance, while trading venues and participants must synchronize clocks used to record reportable events.

Official sources: FCA SYSC 9—Recordkeeping and FCA MAR 5A—Organised Trading Facilities

8. SEBI Market and Cyber-Resilience Requirements

Jurisdiction: *India* **|** ***Relevance:*** *Direct*

The Securities and Exchange Board of India has established clock-synchronization, audit-trail and cyber-resilience requirements for regulated securities-market entities. These include synchronization of trading-system clocks, monitoring of security logs and verification of time synchronization among security-monitoring components.

Official sources: SEBI Trading Software and Technology Requirements and SEBI Cybersecurity and Cyber-Resilience Circular

DATA PROTECTION AND PRIVACY

9. EU and UK General Data Protection Regulations

Jurisdiction: *European Union, European Economic Area and United Kingdom* **|** ***Relevance:*** *Strong*

The EU and UK GDPR frameworks require organizations to maintain appropriate security, document qualifying personal-data breaches and demonstrate compliance with applicable data-processing principles. Reportable breaches generally must be notified within 72 hours after awareness.

Verifiable chronology can help establish when unauthorized activity occurred, when it was discovered and when investigation, notification and remediation actions were taken. Personal information should not ordinarily be written directly to an immutable public ledger.

Official sources: EU General Data Protection Regulation and UK Information Commissioner's Office—Personal Data Breaches

10. Other National Data-Breach Requirements

Jurisdiction: *Australia, Singapore and Brazil* **|** ***Relevance:*** *Strong*

Several national privacy regimes impose time-sensitive breach-assessment and notification obligations:

- Australia's Notifiable Data Breaches scheme requires covered organizations to assess suspected eligible breaches and notify the regulator and affected individuals when serious harm is likely.
- Singapore requires notification of qualifying breaches as soon as practicable and no later than three calendar days after determining that a breach is notifiable.
- Brazil's LGPD and its implementing rules require notification of security incidents that may create relevant risk or harm.

Reliable chronology can help document discovery, assessment, containment, notification and remediation.

Official sources: Australia—Notifiable Data Breaches Scheme and Singapore—Data-Breach Notification and Brazil—Security Incident Reporting

CYBERSECURITY AND OPERATIONAL RESILIENCE

11. NIS2 Directive

Jurisdiction: *European Union* **|** ***Relevance:*** *Strong*

NIS2 requires covered essential and important entities to report significant cybersecurity incidents through a staged process. This generally includes an early warning within 24 hours, an incident notification within 72 hours and a final report after the incident has been addressed.

Official source: Directive (EU) 2022/2555—NIS2

12. EU Cyber Resilience Act

Jurisdiction: *European Union* **|** ***Relevance:*** *Strong*

The Cyber Resilience Act establishes cybersecurity requirements for products with digital elements. Manufacturers must report actively exploited vulnerabilities and severe security incidents through specified notification stages, including early warnings subject to defined deadlines.

Official source: Regulation (EU) 2024/2847—Cyber Resilience Act

13. APRA Prudential Standards CPS 230 and CPS 234

Jurisdiction: *Australia* **|** ***Relevance:*** *Strong*

CPS 230 requires regulated entities to identify, escalate, record and address operational incidents and near misses. CPS 234 establishes information-security requirements and associated incident-notification obligations. Qualifying incidents under both standards may be subject to reporting periods measured from the organization's awareness of the event.

Official sources: APRA CPS 230—Operational Risk Management and APRA CPS 234—Information Security

HEALTHCARE, PHARMACEUTICALS AND LIFE SCIENCES

14. FDA 21 CFR Part 11

Jurisdiction: *United States* **|** ***Relevance:*** *Direct*

For covered electronic records, 21 CFR Part 11 requires secure, computer-generated, time-stamped audit trails that independently record the date and time of actions that create, modify or delete records. Changes must not obscure previously recorded information, and audit-trail documentation must be retained and available for agency review.

Official source: 21 CFR § 11.10—Controls for Closed Systems

15. HIPAA Security Rule

Jurisdiction: *United States* **|** ***Relevance:*** *Strong*

The HIPAA Security Rule requires covered entities and business associates to implement mechanisms that record and examine activity in systems containing electronic protected health information. It also requires policies and procedures protecting that information from improper alteration or destruction.

Official source: 45 CFR § 164.312—Technical Safeguards

ELECTRONIC RECORDS AND TRUST SERVICES

16. eIDAS Regulation

Jurisdiction: *European Union* **|** ***Relevance:*** *Direct*

The eIDAS Regulation establishes a legal framework for electronic timestamps. A qualified electronic timestamp receives a presumption concerning the accuracy of the date and time it indicates and the integrity of the data to which it is bound. It must use an accurate time source linked to Coordinated Universal Time and bind time to data so that undetected changes are reasonably prevented.

Clockchain does not automatically constitute a qualified electronic timestamp under eIDAS. Qualification requires compliance with the regulation's specific technical, organizational and trust-service requirements.

Official source: Regulation (EU) No 910/2014—eIDAS, Articles 41 and 42

STANDARDS AND INDUSTRY FRAMEWORKS

The following are government or industry standards rather than generally applicable legislation. Their legal, regulatory or contractual effect depends on the organization and its operating environment.

17. NIST Special Publication 800-53, Revision 5

Jurisdiction: *United States; used internationally* **|** ***Relevance:*** *Direct*

NIST SP 800-53 includes controls for audit-event generation, audit-record content, timestamping, protection of audit information and record retention. Control AU-8 addresses timestamps, while AU-8(1) addresses synchronization with an authoritative time source.

Official source: NIST SP 800-53 Revision 5

18. PCI Data Security Standard

Jurisdiction: *International* **|** ***Relevance:*** *Direct*

PCI DSS requires covered payment-card environments to log specified security events, protect audit data and maintain consistent time settings across relevant systems. Version 4 addresses synchronization of system clocks through time-synchronization technology.

Official source: PCI Security Standards Council

USING THIS APPENDIX

The regulations and standards identified here do not generally require the use of Clockchain, blockchain technology or any particular external time-verification service. Their relevance arises from the importance they place on one or more of the following:

- accurate timestamps and synchronized clocks;
- time-stamped audit trails;
- integrity and retention of electronic records;
- traceability of automated decisions;
- reconstruction of transactions or system activity;
- documentation of cybersecurity and privacy incidents; and
- compliance with time-limited reporting obligations.

Clockchain may support these functions by providing an independently verifiable chronology against which digital events and internally generated records can be compared.

The applicability of any requirement depends on the organization, its activities, its jurisdiction and the systems involved. Organizations should obtain appropriate legal, regulatory and technical advice before relying on verifiable time as part of a compliance program.