Empowering Auditor Compliance: DIRO’s Alignment with PCAOB’s AS 2310: The Auditor’s Use of Confirmation

Internet Original Documents, Inc. (DIRO)

Last Updated: May 12, 2025

Table of Contents:

1. Executive Summary

The PCAOB's updated AS 2310: The Auditor's Use of Confirmation, modernizes the confirmation process to address rising cyber-fraud and inefficiencies in traditional methods like paper-based confirmations. Effective for fiscal years ending on or after June 15, 2025, AS 2310 mandates auditors to confirm cash and accounts receivable (A/R) balances or obtain equivalent audit evidence through direct, auditor-controlled access to external sources. Silence is no longer acceptable as agreement, and auditors must rigorously document reliability and control over confirmation processes.

DIRO's patented technology delivers "direct access" (AS 2310 §.24) at scale by **cryptographically locking the live source with its data** and anchoring a SHA‑3 hash on a public blockchain. The resulting DIRO is immutable, independently verifiable, and fully detached from company IT environments, satisfying every reliability criterion in AS 2310 and AS 1105: Audit Evidence, as more efficient and superior evidence over traditional confirmation channels (mail, e‑mail, fax, portal correspondence).

The evidence provided is independent and directly from the original source, as the confirming party leverages a terminal providing read-only access by DIRO as the intermediary, as a reliable and independent facilitator for original documents and data globally.

Key Takeaway: DIRO empowers auditors to meet AS 2310's requirements for confirmations with real-time, tamper-proof evidence, reducing fieldwork time and enhancing audit reliability.

2. Regulatory Context: Why AS 2310 Was Modernized

The PCAOB updated AS 2310 to address challenges in traditional confirmation processes:

- **Inefficiency**: Paper-based confirmations are slow and misaligned with modern financial close cycles.

- **Cyber-Fraud Risks**: Increasing threats of interception and alteration necessitate auditor control over evidence channels.

- **Non-Responses**: Silent non-responses are no longer acceptable as audit evidence, requiring proactive follow-up or alternative procedures.

- **Technology Enablement**: Technology-neutral language allows secure digital portals, provided that the auditors control access and evaluate reliability (Appendix B).

Appendix B explicitly permits intermediaries like DIRO for confirmations, provided auditors maintain control, assess intermediary reliability, and ensure no company override. Appendix C allows alternative evidence, such as viewing balances on secure websites, to be as persuasive as confirmations if auditor-controlled.

Key Takeaway: AS 2310 encourages auditor-controlled digital solutions for confirmations, making DIRO's technology a compliant and efficient choice.

3. Key AS 2310 Requirements for Auditors

Auditors performing confirmations under AS 2310 must address the following:

Clause	Theme	Practical Obligation
§.24	Cash and A/R Evidence	Confirm cash and A/R or obtain equivalent evidence via direct access to external sources.
§.14-.17	Auditor Control	Ensure direct communication or use reliable intermediaries, preventing company alteration.
Appendix B (§.B1-.B2)	Intermediary Controls	Evaluate design and operating effectiveness of controls to mitigate interception, alteration, and company override risks.
Appendix C	Alternative Procedures	Use auditor-controlled access to secure websites as persuasive evidence if confirmations are impractical.

Key Takeaway: Auditors must maintain control, ensure evidence reliability, and document processes rigorously for confirmations.

4. DIRO Technology Overview

DIRO’s technology enables auditors to obtain confirmations directly from, e.g., financial institutions, ensuring compliance with AS 2310. The process involves three steps:

Step 1 – Impersonation Check and Capture at Source

- Auditors initiate a DIRO session in a shielded virtual machine (VM) terminal with read-only access.
- The company logs in using its credentials (e.g., BankID with MFA/2FA) to access the bank’s portal.
- In a controlled and tamperproof environment, DIRO captures live HTML, DOM, PDF, SSL/TLS certificate fingerprints, HTTP response headers, and forensic metadata, ensuring authenticity via a whitelist of trusted financial institutions.

Step 2 – Hash and Anchor

- DIRO computes a SHA-3 hash of the captured data, including provenance metadata (URL, timestamp, certificate, etc).
- The hash is anchored on a public blockchain in near real-time, ensuring immutability and tamper resistance.

Step 3 – Deliver Internet Original Document as Evidence

- A tamper-evident PDF or JSON-LD package is generated, containing the data, metadata, and blockchain transaction ID.
- Any alteration breaks the hash, guaranteeing evidence integrity for audit workpapers.

Key takeaway: DIRO’s auditor-controlled, cryptographically secure process delivers immutable confirmation evidence, integrable with existing audit toolkits via APIs or exports.

5. Mapping DIRO to AS 2310 Requirements

DIRO's technology aligns with AS 2310's requirements for confirmations, as shown below:

AS 2310 Criterion	DIRO Capability	Evidence File
External source and auditor control (§. 24)	Auditor controls the DIRO session environment (tamperproof); company credentials can not be used to modify or alter.	Internet Original Document; provenance, audit log.
Risk of interception/ alteration (App. B §.1)	End-to-end TLS; hash anchored on blockchain; immutable PDF.	Hash-verify, digital package; blockchain TX ID.
Independence from company override (App. B §.2)	DIRO is contracted by the auditor; company has no administrative control over the platform.	Engagement contract; access logs.
Intermediary control evaluation (App. B §.2)	SOC 2 Type II, ISO 27001; annual bridge letter.	SOC report; audit file.
Documentation and retention (AS 1215)	Internet Original Document embeds metadata, hash, TX ID; exportable to long-term archive.	Workpapers cross-referenced to audit schedules.

Key takeaway: DIRO exceeds AS 2310's reliability and control thresholds, providing auditors with robust, inspection-ready evidence for confirmations.

6. Control Evaluation and Compliance Certifications

DIRO's 2024-25 SOC 2 Type II report (available under NDA) and ISO 27001 certification cover critical controls for AS 2310 compliance:

- **CC6.1 – Logical Access Controls**
  Role-based access control (RBAC), enforced multi-factor authentication (MFA), no shared credentials.
  ✔️ *Ensures only authorized personnel can access production systems.*

- **CC7.1–CC7.4 – System Operations, Change Management, and Vulnerability Management**
  Signed software releases with audit trail, CI/CD deployment controls, semi-annual CREST-certified penetration tests, CVSS-based patching policy.
  ✔️ *Monitors for unauthorized changes and system threats.*

- **A1.2 – Transmission of Information**
  All data in transit is secured using mutual TLS 1.3; HTTP Strict Transport Security (HSTS) headers are enforced.
  ✔️ *Prevents interception and downgrade attacks.*

- **A1.4 – Integrity of Data Inputs and Outputs**
  Captured content is SHA‑3 hashed and blockchain-anchored; DIRO provides a verification API to check provenance and tamper-resistance.
  ✔️ *Protects evidence from silent tampering or replacement.*

- **A1.5 – System Availability**
  Backed by ≥ 99.9 % uptime SLA; hosted across redundant AWS regions with failover and auto-scaling.
  ✔️ *Ensures continued access for auditors and clients.*

Key takeaway: DIRO’s controls directly address AS 2310’s Appendix B requirements for intermediary reliability, safeguarding confirmation evidence.

7. Frequently Asked Questions

Q 1. Is portal evidence truly as persuasive as a traditional confirmation?

Yes, Appendix B of AS 2310 explicitly states that auditor-controlled access to secure portals (e.g., DIRO) is as persuasive as traditional confirmations, provided reliability is evaluated. DIRO’s cryptographic controls enhance evidence integrity.

Q2. How does DIRO ensure independence from the audited company?

DIRO is contracted by the auditor, and companies have no administrative control. Read-only access via company credentials ensures no override capability, per Appendix B (§.2).

Q 3. Does blockchain anchoring raise GDPR concerns for confirmations?

No, only a SHA-3 hash (256-bit non-personal data) is stored on-chain, ensuring no PII exposure and GDPR compliance.

Q4. How does DIRO support global financial institutions?

DIRO has whitelisted over 50,000 trusted sources in over 195 countries, enabling auditors to access data from any financial institution with a secure, consent-based login. Backed by its patented technology, DIRO offers the broadest verified access to financial institutions worldwide in real time.

Q 5. How does DIRO's patented technology differ from traditional methods?

DIRO captures the downloaded document, HTML and the underlying SSL cert, and forensic metadata, then anchors a hash of the entire package on a blockchain, whereas traditional methods lack provenance and immutability.

8. Conclusion

With traditional confirmation channels constrained and AI‑generated forgeries on the rise, auditors need a secure, inspection‑ready method to obtain external evidence. **DIRO's Internet Original Document provides a cryptographically locked, auditor‑controlled path that squarely meets PCAOB's AS 2310 framework.** By integrating DIRO into cash and A/R work programs today, auditors can accelerate fieldwork, cut confirmation costs, and enter the 2025 inspection cycle with confidence.

For more information, visit:

DIRO website: https://diro.io/

DIRO Trust Center: https://trust.diro.io/

How it works: https://diro.io/how-it-works/

Global coverage: https://diro.io/see-coverage/

Contact:

Per Jirstrand

CEO | DIRO

Email: per@diro.io