

# Confirmation Letter in CPA Practice

## Current PCAOB and GAAS Requirements: Key Changes in 2024–2026

**T**he confirmation letter is a fundamental audit evidence tool in CPA practices. Here, we'll focus on the revised PCAOB AS 2310 (effective June 15, 2025) and the AICPA Proposed SAS on External Confirmations (February 2025) to help practitioners who need to update their processes ahead of the new standards.

Topics covered include the legal nature of confirmation letters, their classification by form and application area, a detailed analysis of material 2024–26 regulatory changes across PCAOB and GAAS, the critical Direct Access principle, digitization risks and opportunities, workflow adaptation steps, common inspection deficiencies, and the impact on auditor liability.

### 1. Confirmation Letter: Legal Nature and Evidentiary Status

A confirmation letter (external confirmation) is audit evidence obtained directly by the auditor from an independent third party, such as a bank, accounts receivable debtor, legal counsel, broker or custodian. The operative word is “directly.” If the response is routed through the client, it loses its status as external confirmation regardless of its content (PCAOB AS 2310; ISA 505).

In the hierarchy of audit evidence reliability under PCAOB AS 1105 and ISA 500, external confirmations rank among the highest, alongside the auditor’s own physical observation. This elevated status reflects one foundational premise: an independent third party with no financial interest in the client’s reporting outcomes is a more reliable source of information than the client itself.

That same reliability, however, makes confirmation fraud a highly attractive scheme. The Wirecard collapse (Germany, 2020) remains the starkest modern example: auditors received fabricated bank confirmations via a chain of intermediaries fully controlled by the client, confirming €1.9 billion in cash that did not exist. The Luckin Coffee fraud (2019–20) used similar logic in accounts receivable. These cases, and a string of regional

bank failures, were direct catalysts for the regulatory overhaul described in this article.

### 2. Classification of Confirmation Letters

#### 2.1 By Request Form

*Positive Confirmation:* A positive confirmation request requires the respondent to reply in all cases, regardless of whether they agree or disagree with the information presented. This is the preferred form under current standards for any account with a risk of material misstatement. Two sub-variants exist:

- **Filled-form:** the auditor states the balance or condition and asks the respondent to confirm or dispute it. Efficient, but carries the risk of respondents confirming without careful review.
- **Blank-form:** the auditor asks the respondent to provide the data independently, without a suggested figure. Considered more reliable because it eliminates “rubber-stamp” agreement as the respondent must actively retrieve and state their own records.

*Negative Confirmation:* A negative confirmation request asks the respondent to reply only if they disagree with the stated information; silence is treated as implied agreement. This is historically used for large populations of small, low-risk balances, such as individual retail customer accounts. Following the 2024–25 regulatory reforms, this form has been severely restricted under PCAOB and is outright prohibited under ISA (UK) 505 (FRC, effective Dec. 15, 2024). Any continued use under PCAOB requires explicit, documented justification tied to a demonstrated low-risk assessment.

#### 2.1 By Area of Application

*Bank Confirmation:* This is the most widely used type in financial statement audits. The auditor requests confirmation from the client’s banks of deposit account balances, outstanding loan balances and terms, credit facility availability, collateral pledged, letters of credit, and guarantees. The standardized bank confirmation form in the United States was developed jointly by the American Bankers Association (ABA) and the AICPA. Under the revised PCAOB AS 2310 (effective June 15, 2025), confirmation of all cash and cash equivalents held at third parties is now a mandatory procedure, not merely a recommended best practice.

*Accounts Receivable Confirmation:* Auditors send requests to the client’s customers to confirm the balance owed as of the

Document	Response Source	Evidence Reliability	Governed By
Confirmation Letter	Independent 3rd party → auditor directly	External - High	AS 2310 / ISA 505
Mgmt. Representation Letter	Client management → auditor	Internal - Mandatory but limited	AS 2805 / ISA 580
Client’s internal documents	Client	Internal - Moderate	AS 1105 / ISA 500
Oral management representations	Client (verbal)	Minimal - Not standalone	AS 2805 / ISA 580
Auditor’s direct observation	Auditor personally	Direct - Highest	AS 1105 / ISA 500

audit date. This is a primary procedure for trade receivables and is directly affected by the restriction on negative confirmations: accounts receivable populations that were historically confirmed via negative form must now be re-evaluated, with positive confirmations used for material or higher-risk balances.

**Legal Confirmation:** Requests to the client’s external legal counsel to confirm pending or threatened litigation, claims, and assessments, along with counsel’s assessment of likely outcomes and materiality. Governed separately by PCAOB AS 2505 (Inquiry of a Client’s Lawyer Concerning Litigation, Claims, and Assessments). This category is not materially affected by the AS 2310 reform, as it operates under its own standard.

*Other Types*

- **Investment/Custodian Confirmation:** Securities holdings, fund balances, and managed account details confirmed by brokers and custodians.
- **Inventory Confirmation:** Goods held at third-party warehouses, bonded facilities or on consignment.
- **Insurance Confirmation:** Policy terms, coverage limits and premiums from insurers.
- **Management Representation Letter (MRL):** A distinct category in which management itself is the confirming party. Mandatory under AS 2805/ISA 580 but cannot substitute for independent external confirmations; it documents management’s acknowledgment of its responsibilities and the completeness of information provided.

### 3. 2024–2026 Regulatory Reforms: Detailed Analysis

#### 3.1 PCAOB AS 2310—‘The Auditor’s Use of Confirmation’

**Adopted:** December 2023 (SEC approved). **Effective:** Audits of fiscal years ending on or after June 15, 2025.

The previous PCAOB confirmation standard was over 30 years old, written in an era of paper letters and fax machines, and had not been substantively updated since PCAOB’s inception in 2003. A decade of inspection findings, combined with high-profile frauds in which falsified confirmations were central, made reform urgent. The new AS 2310 adopts a principles-based architecture applicable to both paper and digital confirmation processes.

Six Core Changes Under PCAOB AS 2310	
①	<b>CASH CONFIRMATION—NOW MANDATORY</b> Confirmation of all cash and cash equivalents held at third parties is elevated from best practice to a required procedure. Auditors must either send a direct bank request or obtain independent access to bank data via a verified digital channel.
②	<b>RISK ASSESSMENT INTEGRATION (AS 2101/AS 2301)</b> Confirmation planning must be explicitly linked to the identification and assessment of risks of material misstatement. Auditors must document how the selection of items to confirm responds to the specific risks identified in the engagement.
③	<b>EXPANDED EXCEPTION DOCUMENTATION</b> Every discrepancy received must be analyzed through the lens of fraud risk, not merely attributed to timing differences or client error. Documentation requirements are explicit.
④	<b>AUDIT COMMITTEE COMMUNICATION</b> Management refusal to authorize confirmation requests, or receipt of unreliable or restricted responses, triggers a mandatory communication to the audit committee.
⑤	<b>DIGITAL CONFIRMATIONS—EXPLICITLY REGULATED</b> Reliability standards apply equally to paper letters, web portals, APIs and all other electronic channels. The principles governing independence and direct access are technology-neutral.
⑥	<b>NEGATIVE CONFIRMATIONS—SUBSTANTIALLY RESTRICTED</b> Use requires explicit documented justification. Permissible only when the risk of material misstatement is demonstrably low and specific documented conditions are met.

#### 3.1 AICPA - Proposed SAS ‘External Confirmations’ (February 2025)

**Published:** Feb. 27, 2025 (Exposure Draft, AICPA ASB). **Proposed effective date:** Periods ending no earlier than Dec. 15, 2027.

The AICPA Auditing Standards Board governs audit standards for non-issuers: private companies, nonprofits, employee benefit plans and governmental entities. The proposed SAS amends three existing standards—AU-C 330, AU-C 500 and AU-C 505—and brings non-issuer audits broadly into alignment with PCAOB’s revised approach, while maintaining the GAAS tradition of principles-based guidance

- **Intermediary rules:** when confirmation platforms or aggregators are used, auditors must assess and document their reliability as a channel, including how they authenticate respondents and protect response integrity.
- **Direct access clarified:** credentials or access tokens provided by the client do not constitute “direct” access for confirmation purposes. Data obtained via client-provided access may be considered alternative

audit evidence under AU-C 500, but not as a confirmation.

- **Government agencies as confirming parties:** tax authorities, licensing bodies and regulatory agencies are explicitly recognized as valid external confirming parties, particularly relevant for governmental and not-for-profit audits.
- **Cash confirmation mandate:** mirrors PCAOB’s approach—confirmation of cash balances held at financial institutions becomes a required procedure.

Parameter	PCAOB AS 2310	AICPA SAS (Proposed)
Scope	Public issuers (SEC registrants)	Non-issuers (private, NFP, gov’t)
Effective date	June 15, 2025	Dec. 15, 2027 (proposed)
Cash confirmation	Mandatory (new requirement)	Mandatory (proposed)
Negative confirmations	Restricted - documented justification required	Restricted - principles-based
Digital channels	Explicitly regulated	Explicitly regulated
Intermediary platforms	Independence assessment required	Reliability assessment required
Audit committee reporting	Required (on refusals/unreliable responses)	Recommended
Approach	Rules-based + principles	Principles-based (GAAS tradition)

### 4. The Direct Access Principle: The Foundation of Confirmation Reliability

Both AS 2310 and ISA (UK) 505 converge on a single foundational principle: the reliability of a confirmation is not determined by the format of the document, but by the independence of the channel through which it is received. The auditor must maintain unbroken control of the entire chain—from the dispatch of the request to the receipt of the response—without the client intervening at any point.

This principle has significant practical implications in the digital environment, where the boundaries between “auditor-controlled” and “client-provided” access are often blurred. A bank portal accessed through credentials shared by the client, for example, does not meet the direct access standard, even if the data retrieved appears complete and accurate. The auditor has no independent assurance that the portal is genuine, that the data has not been manipulated at the source or that all accounts are visible.

### 4.1 Assertions Coverage in Digital Confirmations

A critical and frequently overlooked issue is digital confirmations, particularly API-based responses from bank portals, which may address certain audit assertions while leaving others uncovered. An API response confirming the balance on a specific account addresses existence and valuation but says nothing about completeness: it does not reveal whether additional accounts exist that the client has not disclosed. Auditors must explicitly identify which assertions are covered by each digital confirmation received and design supplementary procedures to address any gaps.

#### Direct Access Checklist for Digital Confirmations

- X Response routed through the client (even unaltered) - NOT a valid external confirmation.
- X Portal access via credentials provided by the client - NOT direct access.
- X Confirmation received via the client's email account or document management system - NOT valid.
  
- ✓ Auditor independently registers with and authenticates to the confirming party's platform.
- ✓ Auditor independently verifies the URL and SSL certificate of the digital platform used.
- ✓ Auditor documents which assertions are covered by the digital response, and which require additional procedures (particularly: completeness for bank accounts, inventory, receivables).
- ✓ Auditor retains electronic evidence of the confirmation response in the workpapers, including timestamp, authentication log, and response metadata.

## 5. Digitization of the Confirmation Process: Opportunities and Risks

### 5.1 The Rise of Digital Confirmation Platforms

Specialized digital confirmation platforms such as Confirmation.com (Thomson Reuters), Circit and CCH Axxess Validate have become the dominant channel for bank confirmations in most developed audit markets. These platforms use multi-factor authentication, digital signatures and encrypted transmission to address many of the vulnerabilities inherent in paper-based processes. Response times have shortened from two to three weeks (paper mail) to 24–72 hours. PCAOB AS 2310 and ISA (UK) 505 both explicitly accommodate digital confirmation channels, applying the same reliability principles regardless of medium.

### 5.2 Risks Specific to Digital Channels

Digitization introduces new categories of risk that auditors must actively manage:

- **Spoofed portals and phishing:** A sophisticated client or co-conspirator can create a replica of a bank's confirmation portal. The auditor who does not independently verify the URL and authentication certificate may receive a fabricated response. This is a documented threat vector, not a theoretical one.
- **Man-in-the-middle attacks:** Encrypted channels notwithstanding, interception between the bank's system

and the auditor's interface remains a risk, particularly where platforms rely on email notification links rather than direct login authentication.

- **Intermediary platform risk:** even legitimate aggregator platforms sit between the auditor and the confirming party. AS 2310 and the AICPA Proposed SAS both require auditors to assess whether the use of an intermediary compromises the “direct” nature of the access.
- **Incomplete assertion coverage:** as noted in Section 4, API-based responses often confirm specific account details without providing assurance on completeness, a gap that must be explicitly addressed in the audit program.

### 5.3 Emerging Technologies: AI and Distributed Ledger

The International Auditing and Assurance Standards Board (IAASB)'s ongoing projects on ISA 330, ISA 500 and ISA 520 (with first full drafts expected at its March 2026 board meeting) place significant emphasis on the technological transformation of audit evidence gathering. Two technologies are attracting particular regulatory attention:

- AI-assisted confirmation analysis: tools that automatically scan received confirmations for anomalies, match digital signatures against known registries, and flag statistical outliers in response patterns.
- Second, distributed ledger technology (blockchain): in principle, shared immutable ledgers maintained by banks and their auditors could provide real-time, tamper-proof balance data, rendering the traditional request-response cycle obsolete.

Both remain in early-stage regulatory consideration, but CPAs should monitor these developments as they will reshape confirmation practice in the medium term.

## 6. Managing Non-Responses, Exceptions and Management Refusals

### 6.1 Non-Responses Platforms

When a confirming party does not respond to a positive confirmation request, AS 2310 is unambiguous: the auditor cannot treat silence as agreement (that is the logic of negative confirmations, now restricted). The auditor must either obtain a second response or perform alternative audit procedures sufficient to address the same assertions.

Acceptable alternatives include examination of subsequent cash receipts, review of shipping documents and sales invoices, or analysis of customer correspondence. The nature and results of all alternative procedures must be documented in the workpapers.

A pattern of non-responses, particularly in specific customer segments, geographic regions, or time periods, is itself a potential fraud indicator and must be evaluated as such under the expanded exception documentation requirements of AS 2310.

### 6.2 Exceptions and Discrepancies

Under revised AS 2310, every discrepancy between the amount stated in the confirmation request and the amount confirmed by the respondent must be analyzed through the lens of fraud risk, not merely attributed to a timing difference or client error. The auditor is required to:

1. Investigate the nature of the discrepancy by obtaining an explanation from the client and, where appropriate, the respondent.
2. Evaluate whether the explanation is consistent with the auditor's understanding of the client's business and the results of other procedures.
3. Consider whether the discrepancy—individually or in aggregate with other exceptions—indicates a risk of material misstatement due to fraud.
4. Document all of the above explicitly in the workpapers, including the auditor's conclusion on fraud risk implications. Auditors must also be alert to "soft" exceptions: responses that are qualified, restricted or accompanied by legal caveats. A bank that confirms a balance "subject to verification" or "as of a date other than requested" has not provided a clean confirmation, and the auditor must assess what additional work is required.

### 6.3 Management Refusal to Authorize Confirmations

When management declines to grant the auditor permission to send confirmation requests, for example, citing confidentiality concerns or business relationship sensitivities, this is a significant red flag. AS 2310 prescribes a structured response: assess whether the refusal is reasonable; perform alternative procedures; evaluate the impact on assessed fraud risk; consider implications for the auditor's report; and communicate the situation to the audit committee. An unexplained or unreasonable refusal to permit bank confirmations, in particular, should elevate the auditor's skepticism substantially and may ultimately affect the audit opinion.

## 7. Practical Recommendations: AICPA Transition Plan

The following plan is designed for CPA firms auditing non-issuers (private companies, nonprofits, and EBP) to align with the proposed updates to AU-C 330, 500, and 505:

1. **Audit current practices.** Review recent engagements for use of negative confirmations (and whether conditions for their use are still met); cases where responses were obtained through the client; and instances where non-responses were not followed up with alternative procedures.
2. **Adopt the Presumptively Mandatory Cash Rule.** Update audit programs to require bank confirmations for significant cash and cash equivalent balances. Unlike the PCAOB's blanket mandate, the AICPA allows you to skip cash confirmation if you document that it's ineffective or if the account is not a "significant" balance/assertion.
3. **Transition to positive confirmations.** Identify all account populations where negative confirmations were previously used and redesign the confirmation strategy. For material or higher-risk balances, positive blank-form confirmations are the preferred approach.
4. **Redesign confirmation request templates.** Each template must: (a) clearly identify the auditor as the direct recipient of the response; (b) specify the relevant assertions being addressed; (c) include auditor-controlled contact information only; and (d) set a clear response deadline.
5. **Implement or upgrade a digital confirmation platform.** Select a platform with multi-factor authentication, respondent identity verification, and an immutable audit

trail. Establish auditor-controlled accounts independent of client credentials.

6. **Update exception protocols.** Create or revise workpaper templates that require explicit fraud risk evaluation for every discrepancy, not just a client explanation. Ensure senior review before exceptions are closed.
7. **Train engagement teams.** Conduct targeted training on: the presumptively mandatory cash requirement; the direct access principle and its digital implications; the restricted scope of negative confirmations; and expanded exception documentation requirements.
8. **Communicate with those charged with governance.** Update manuals for cases where management refuses to allow a confirmation. The new AICPA guidance requires the auditor to evaluate the implications on the Risk of Fraud and perform alternative procedures that provide "equally persuasive" evidence.

## 8. Practical Recommendations: AICPA Transition Plan

### 8.1 PCAOB and FRC Inspection Findings (2022–25) Platforms

Deficiency	Regulatory Source	Consequence
Response routed through the client	PCAOB Inspections; FRC Reports 2023	Reclassified as non-confirmation; evidence gap
Negative conf. without documented justification	PCAOB Staff Guidance 2024	Insufficient evidence; potential restatement risk
No follow-up on non-responses	FRC Annual Review 2024; PCAOB	Standard violation; unaddressed fraud vulnerability
Digital response misses completeness assertion	AS 2310 §.08; ISA (UK) 505	Undetected undisclosed accounts or balances
Exception not analyzed for fraud risk	AS 2310; PCAOB inspections 2024	Professional liability; regulatory sanction risk
Qualified response accepted without assessment	AS 2310; ISA 505	Unreliable evidence accepted as sufficient
No audit committee communication on refusals	AS 2310 (new requirement)	Non-compliance with mandatory disclosure rule

### 8.2 Auditor Liability Considerations

The regulatory tightening of 2024–2026 has direct implications for professional liability.

First, the elevation of cash confirmation to a presumptively mandatory procedure means that failure to confirm significant bank balances, without a robust, documented "basis for determination," will be extremely difficult to defend in litigation or peer review.

Second, the explicit requirement to perform a fraud risk evaluation for every confirmation exception shifts the burden of proof. An auditor who dismisses a discrepancy as a timing difference without documented evidence of this evaluation will have a weak defense if that discrepancy is later identified as a "red flag" for fraud.

Third, the requirement to communicate with those charged with governance (TCWG) creates a permanent record. If an auditor fails to report a management refusal and a fraud is subsequently discovered, then that omission will be a focal

**Regulators are moving** from procedural compliance to evidence quality. Each confirmation request must be designed around specific audit assertions, each channel must be assessed for independence, and each exception must be evaluated for fraud risk implications.

point in any disciplinary or civil proceeding. CPAs should ensure their professional liability coverage is reviewed in light of these expanded obligations, and that firm-level quality management systems (per AICPA SQMS No. 1, effective Dec. 15, 2025) explicitly address compliance with the new confirmation protocols.

### 9. Conclusion

The PCAOB AS 2310 reform (2025) and the AICPA Proposed SAS on External Confirmations (2027) represent the most significant overhaul of confirmation standards in the United States in more than three decades. They share a common regulatory logic: the reliability of a confirmation is determined not by the form of the document, but by the independence of the channel through which it is received and the completeness of the audit assertions it addresses.

For every practicing CPA, three changes require immediate attention.

- First, cash confirmation is no longer best practice, it is a mandatory procedure under PCAOB AS 2310 (effective June 15, 2025) and a presumptively mandatory procedure under the proposed AICPA SAS (effective Dec. 15, 2027).
- Second, negative confirmation is effectively being retired from professional use: under both frameworks, its conditions for permissible application are now so narrow that most prior uses will not survive scrutiny.
- Third, digital confirmation channels, while offering significant efficiency gains, carry their own independence and completeness risks that must be actively managed and documented, with the AICPA specifically codifying direct access as a valid confirmation medium.

The broader trajectory is clear: regulators are moving from procedural compliance to evidence quality. Each confirmation request must be designed around specific audit assertions, each channel must be assessed for independence, and each exception must be evaluated for fraud risk implications. Firms that build these requirements into their standard methodology, rather than treating them as add-ons to legacy processes, will be better positioned for PCAOB inspections or AICPA peer reviews, better protected against liability and better equipped to deliver audits that meet the profession's public interest mission.

### Key Regulatory Sources

PCAOB AS 2310, The Auditor's Use of Confirmation (Release No. 2023-008; effective June 15, 2025)

AICPA ASB, Proposed SAS: External Confirmations (Exposure Draft, February 27, 2025)

PCAOB AS 1105, Audit Evidence

PCAOB AS 2101, Audit Planning | AS 2301, The Auditor's Responses to the Risks of Material Misstatement

PCAOB AS 2805, Management Representations | AS 2505, Inquiry of a Client's Lawyer

PCAOB QC 1000, A Firm's System of Quality Control (effective December 15, 2025)

PCAOB Staff Audit Practice Alert - Guidance on AS 2310 (2024)

PCAOB, 2025 Inspection Priorities Spotlight (December 2024)

FRC, ISA (UK) 505 (Revised October 2023) - comparative reference for digital channel standards

IAASB, ISA 330 / ISA 500 / ISA 520 Revision Projects - First full drafts expected March 2026

Svetlana Gadzhieva, CPA, is a member of the CalCPA Accounting Principles and Assurance Services Committee. You can reach her at <https://gadzhieva.com>.