PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

# SPOTLIGHT

## Observations From the Target Team's 2023 Inspections

September 2024

# CONTENTS

# OVERVIEW

The PCAOB's Division of Registration and Inspections ("staff" or "we") has a target team consisting of inspectors who focus on emerging audit risks and other topics that the staff believes could have important implications for audits and reviews performed by the audit firms we inspect.

Created in 2019, the target team executes in-depth interviews and review procedures to gather information across audit firms. The target team has advanced the PCAOB's mission to protect investors by developing observations across audit firms and communicating those insights to inspected audit firms in order to advance audit quality.

In 2023, the target team focused its procedures on reviewing audits of public companies that included risks related to three areas:

1. **Crypto Assets** – As a result of crypto asset market disruptions and the corresponding emerging risks, the target team performed procedures to gather information about certain audits of public companies with material crypto asset activities. This included obtaining and analyzing information about the audit firms' client acceptance and continuance processes, risk assessment procedures, use of consultation and subject matter groups, guidance and tools, and audit execution, including the extent of procedures conducted by the engagement teams to determine the relevance and reliability of information obtained from blockchains.
2. **Multiple jurisdictions ("multi-location") audits** – In 2019, the target team performed inspection procedures on multi-location audits. The target team's objectives in 2019 included understanding engagement scoping, risk assessment procedures, component auditor reporting, group auditor monitoring, and audit firm-level tools and guidance. Given ongoing geopolitical turmoil and public companies switching from China-based audit firms to those in the U.S., the target team once again selected multi-location audits as a focus area in 2023.
3. **Significant or unusual events or transactions** – The target team's focus included inspection procedures to gain insights into the audit firms' methodologies, practices, and execution of audits involving risks posed by significant or unusual events or transactions ("such events or transactions"). The target team considered, for example, non-recurring end of period events or transactions, events or transactions involving related

## Interim Reviews

When determining the 2023 inspection plan, the target team planned to focus on audits of public companies that include risks related to crypto assets, first-year audits, multi-location audits, and significant or unusual events or transactions. The target team's inspection approach is flexible to specifically allow it to pivot, if and when necessary, to address emerging risks or issues. Given the events in the banking sector that occurred in 2023, the target team changed its plan to focus on the interim reviews of certain banks rather than first-year audits. The observations from the target team's interim reviews can be found in the **"Bank Financial Reporting Audits" Spotlight**, published in September 2024.

parties, complex investment or financing arrangements, and failures to appropriately evaluate the risks and respond to such events or transactions. Examples of such events or transactions reviewed by the target team included cybersecurity events or data breaches, gains or losses from lawsuits, interruptions to operations from natural disasters, and early retirement of debt and/or restructuring.

This Spotlight provides auditors and other stakeholders with a view into the target team's work in 2023, including inspection results that cover examples of deficiencies that resulted in the issuance of comment forms, other observations, and good practices.

# 2023 FOCUS AREAS FOR THE TARGET TEAM

## Crypto Assets

The target team performed review procedures on 11 audits of public companies with crypto asset activity across four U.S. global network firms (GNF).[1] The primary objectives of the inspection procedures performed by the target team were to understand:

1. How did the audit firm plan for increasing levels of crypto asset activity in their audits?
2. Did the audit firm have personnel with the requisite skills to audit crypto asset transactions?
3. How was the engagement team using the audit firm-developed tools, templates, and guidance in audits involving crypto assets?
4. Had the audit firm identified, and was the engagement team using, industry or subject matter groups to support these audits?
5. Were there any consultation procedures in place to support the engagement team's audit procedures?

## Inspection Results

The target team identified the following deficiencies in engagement reviews of five public company audits across three audit firms:

1. **The Auditor's Response to the Risks of Material Misstatement** – Certain engagement teams did not perform sufficient procedures to address the risk of occurrence related to crypto asset customer revenue transactions. For example, the engagement team's tests of details were limited to tracing the third-party customer's crypto asset revenue transactions recorded in the public company's accounting system to its report writing system, which was not in scope for testing. The accounting system was also the source of the data inputs to the report writing system.
2. **An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements** – Certain engagement teams did not obtain sufficient appropriate audit evidence regarding the design and operating effectiveness of controls over the existence, completeness, valuation, rights and obligations, or presentation and disclosure related to safeguarding crypto assets held on behalf of platform users.[2] For example, the

[1] U.S. GNF firms are headquartered in the U.S. and are members of global networks through which they affiliate with audit firms in other countries for various business and client service purposes. Registered public accounting firms provide information about those affiliations in their annual reports on PCAOB Form 2. These U.S. firms are inspected by the PCAOB annually.

[2] In this Spotlight, the term "platform" refers to a) where public companies are providing an online application or systems that bring together buyers and sellers of crypto assets to facilitate transactions or trades and outsources the safeguarding of their customers' crypto assets to a third-party hosted provider, or b) where public companies are providing an online application or system to record these transactions and hold the crypto assets on behalf of their customers.

engagement team did not perform one or more of the following audit procedures:

- Identify and test controls that addressed the risk to the existence of and rights to crypto assets held in cold storage.[3]
- Identify and test controls that addressed the risks related to the existence of unauthorized crypto asset transactions because the engagement team did not review whether configuration settings were properly implemented for an in-scope system in accordance with the public company's authorization policy for crypto asset transactions.
- Evaluate whether the management review control was designed and operating effectively to address the risk of material misstatement, given that certain crypto asset balances and the related variances of those balances were aggregated and assessed on a net basis and were not aggregated individually and on an absolute basis, as specified in the control description.
- Identify and test controls over the accuracy and completeness of the list of imported authorized wallet addresses used in the operation of an automated monitoring application control.
- Sufficiently test information technology general controls (ITGCs) in the domain of Change Management as the engagement team did not evaluate whether changes to the public company's accounting or finance system were tested prior to being implemented into production.
- Sufficiently test access controls for an accounting or finance system, as the engagement team did not identify and test any controls over the accuracy of the user access listing used in the operation of certain controls and did not identify and test any controls that addressed the risk that inappropriate updates were made to the data within the system.
- Sufficiently test ITGCs, and as a result, did not have a basis to conclude that information technology application controls (ITACs) and/or information technology (IT) dependent manual controls were effective.

3. **Audit Evidence** – The target team noted instances where certain engagement teams did not perform sufficient procedures over the information used to test certain controls. For example, the target team noted that engagement teams did not:
   - Test the completeness of the population that was used to select items to test the movements of crypto assets transferred out of cold storage or test any controls over the completeness of the population.
   - Sufficiently test the completeness of the population of system changes from which it selected its samples for testing or sufficiently test any controls over the completeness of the population.
4. **Auditor Reporting of Certain Audit Participants** – The target team noted instances in the Form AP submitted by the audit firm where participation of certain non-U.S. audit participant(s) was not appropriately disclosed, including which participant:
   - Tested crypto asset-related controls.

[3] In this Spotlight, the term "cold storage" refers to storing crypto assets somewhere that is not connected to a network or internet.

- Performed other procedures (e.g., observation of the private key ceremony[4] or testing ITGCs); and/or
- Provided services from a shared service center.

5. **Auditor Independence** – The target team noted an instance where the audit firm did not perform any procedures to determine compliance with standards and rules of the U.S. Securities and Exchange Commission (SEC) and PCAOB, as appropriate, with respect to independence of certain engagement team members that participated in the audit.

## Inspection Observations Related to Crypto Assets

For more observations, including audit deficiencies, good practices, and other reminders related to the audits involving crypto assets, please refer to our June 2023 Spotlight, "**Inspection Observations Related to Public Company Audits Involving Crypto Assets**," and the Investor Advisory, "**Exercise Caution With Third-Party Verification/Proof of Reserve Reports**."[5]

## Observations

The following are other observations specific to crypto assets from public company audits across audit firms. We share these observations to provide further transparency into the audits of companies with material crypto asset activities and certain practices at these companies. The discussion in this section does not indicate noncompliance with PCAOB standards. While these examples were not deemed to be deficiencies, the target team recognized that without other controls, there was a risk that they could have been. The determination of whether an auditor obtained sufficient appropriate audit evidence in support of the auditor's opinion on the financial statements or internal control over the financial reporting should be made based on the facts and circumstances of the particular audit and the company being audited.

1. **ITACs** – For two public company audits reviewed at one audit firm, testing of the ITACs could have been considered audit deficiencies if compensating controls were not identified and tested by the auditor, and found to be designed and operating effectively.
   - For example, an engagement team relied on a control where a public company used an application to perform an automatic reconciliation of the subledger system to third-party data, but the engagement team did not obtain an understanding of the types of errors that could be identified and how errors were resolved before final approval of the reconciliation. The engagement team's testing only focused on the approval confirming that no reconciling items were noted. In this instance, other manual reconciliation controls existed and were tested to address the risk.
   - In another example, the engagement team was informed by the public company that a wallet system automatically and continuously captures purchases and sales activity from

[4] A key ceremony can be used to generate the private key for a crypto asset wallet. For Multiparty Computation (MPC), key ceremonies are used to split parts of keys to participants in a secured manner.

[5] In addition, the following SEC's Statements on safeguarding crypto assets may be helpful: "The Potential Pitfalls of Purported Crypto "Assurance" Work" (July 27, 2023) and the SEC's "Remarks before the 2024 AICPA and CIMA Conference on Banks & Savings Institutions: Accounting for Crypto-Asset Safeguarding Obligations – A Facts-Based Analysis" (September 9, 2024).

the blockchain. Instead of tracing a transaction through from beginning to end to confirm that automatic updates occur, the engagement team's testing focused on reviewing the code, confirming their understanding of how the code works, and then selecting purchases and sales transactions that were already recorded in the subledger and reconciled to the blockchain data. By selecting from sales already recorded in the subledger, the engagement team did not observe if the code that was reviewed supported that the wallet system automatically and continuously captured purchases and sales activities from the blockchain. In this instance, other manual reconciliation controls existed and were tested to address the risks.

2. **Controls Over Private Keys** – For two public company audits reviewed at one audit firm, the target team observed differing approaches to custody the private keys. For one of these audits, the public company maintained custody of the private keys through internally hosted wallets. For the other audit, the public company outsourced the maintenance of the private keys through custodial wallets to a third-party service provider and obtained a related service organization controls report. The engagement team's audit procedures varied based on the public company's approach to custody/maintenance of the private keys.

3. **Risk of Material Misstatement When Using Third-Party Custodians** – For five public companies reviewed across three audit firms, one or more public companies used third parties to maintain custody of crypto assets that they owned or held for their customers. In all instances, the engagement teams evaluated a service organization controls report(s), including the complementary user entity controls relevant to the public companies.

## Reminder: Safeguarding Private Keys

Due to the evolving nature of crypto assets and the importance of safeguarding the private keys, it is important that engagement teams identify and test controls that management has implemented over the prevention or timely detection of unauthorized acquisition, use, or disposition of the public company's assets that could result in a material misstatement of the financial statements, including considerations over the risk of loss, theft, or destruction of the private keys.

For the five audits of public companies that used external custodians, the identified and assessed risks of material misstatement were different from the risks of material misstatement in audits of companies that managed their own custody functions. For example, the target team observed differences in the risks of material misstatement related to the following:

- Safeguarding and management of private key(s).
- Limited, if any, access by employees to those crypto assets.
- Internal controls that use record matching from the public company to those of the outside custodian; and
- Indemnification by the outside custodian stemming from a loss event.

4. **Risk Assessment** – Of the 11 public company audits reviewed, four public company audits across three audit firms

identified significant risks of material misstatement related to the (1) loss due to misappropriation, (2) destruction, or (3) loss of control due to theft (access rights) of private keys associated with crypto asset-related transactions, including one fraud risk.

Of the remaining seven audits of the public companies reviewed, four of those audits did not have material crypto asset balances, and thus the engagement team identified no risk of material misstatement, including fraud, and no additional procedures were performed; two engagement teams determined the risk of material misstatement to be "lower" or "remote" and performed limited audit procedures; and one engagement team concluded the identified risk of material misstatement associated with the crypto assets resided with a third-party custodian and not with the public company. In this last instance, the engagement team considered the risk of material misstatement as remote by reviewing the custodian's contractual obligation to indemnify the public company if it did not safeguard the crypto assets on behalf of the public company's customers.

5. **Audit Firm Risk Assessment Guidance** – One audit firm's guidance stated that there was a presumption that engagement teams would identify a significant risk of material misstatement relating to the potential loss or destruction of private keys.

6. **Critical Audit Matters (CAMs)** – In two of the 11 public company audits inspected, a CAM was identified with respect to crypto asset transactions. In both audits, the CAMs related to auditing the existence and rights and obligations assertions over crypto assets due to the nature and extent of the audit effort required to assess whether the public company controls the private cryptographic keys.

7. **Consultations** – With the exception of one audit firm, all audit firms had a requirement to consult on crypto asset-related transactions based on materiality, first year audits, and/or significant changes related to crypto assets.

   For all public company audits reviewed with material crypto asset balances, engagement teams completed numerous consultations. Some examples of consultations observed by the target team included the following:

   - Principal market determination.
   - Approach to auditing the relevant assertions of crypto assets.
   - Client acceptance.
   - Risk assessment; and
   - Accounting for crypto asset staking.[6]

## Good Practices

The following are good practices that may contribute to audit quality in the execution of engagement procedures on audits of public companies with crypto asset activity:

1. **Use of Specialists or Subject Matter Groups** – While the use of specialists or subject matter experts was not always required by the audit firms' policies, the target team noted that on all public company audits reviewed with material crypto asset balances, the engagement team used auditor-employed specialists or the audit firm's subject matter groups in designing and/or performing audit procedures over crypto asset transactions. These specialists or subject matter groups included pricing desk/services and

[6] In this Spotlight, the term "staking" refers to a process by which individuals lock their crypto assets (their "stake") to support the security and operation of a "proof of stake" blockchain network.

professionals with specialized information technology knowledge with respect to crypto assets.

2. **Engagement Team Staffing** – In three public company audits, senior engagement team members or those with specialized skills performed the audit procedures related to crypto assets.

## Multi-Location Audits

The target team performed procedures on 11 multi-location public company audits across the six GNF audit firms. The 11 public company audits reviewed included public companies with components or operations in China that recently switched from a China-based audit firm to a U.S. audit firm, and audit engagements that used component auditors in China, Russia, Ukraine, Belarus, Gaza, or Israel. Of the 11 public company audits reviewed, 10 included an opinion on the public company's internal control over financial reporting. The primary objectives of the target team's inspection procedures on multi-location audits were to understand:

1. How did engagement teams oversee the work performed by component auditors that may have been faced with challenges because of the pandemic, geopolitical turmoil, or military conflicts in certain locations? Specifically, how did engagement teams oversee the work of component auditors in China, Russia, Belarus, Ukraine, Israel, and the Gaza region?

2. Was audit quality impacted by any staff turnover at component auditors?

3. Were any changes made to audit firm guidance since the target team's review in 2019 that resulted in changes to audit execution of multi-location audits?

4. Were there any updates to firm audit guidance to implement AS 1206, *Dividing Responsibility for the Audit with Another Accounting Firm*, which will be effective for audits of financial statements for fiscal years ending on or after December 15, 2024?

## Inspection Results

At one audit firm, the target team identified deficiencies in the review of two public company multi-location audits related to Form AP. In both audits, the audit firm included inaccurate information in its originally filed Form AP. In one instance, the audit firm miscalculated the aggregate percentage of participation of other audit firms. In another instance, the audit firm included inaccurate information regarding member audit firms that individually represented less than 5% of total audit hours.

## Observations

The following are other observations from the target team's engagement reviews of multi-location audits:

1. **Involvement of Component Auditors** – The group auditor involved component auditors in planning and risk assessment procedures for all public company audits reviewed.

2. **Required Consultations** – For four audit firms, and four public company audits, engagement teams completed firm-required consultations for the audits subject to review. Some examples of required consultation areas included the following:

   - Risk assessment.
   - Principal auditor considerations.
   - Scoping considerations of account significance; and
   - Changes to the materiality benchmark.

3. **Modification of Audit Strategy** – For three audit firms, and six public company audits, the group auditor modified the overall planned audit strategy due to the changes

to the risks of material misstatement. Some examples of new risks identified included:

- Potential impairment charges on assets in Russia.
- De-designation of Russian ruble hedges and asset impairment considerations.
- Identification of a new revenue group of an acquired entity.
- Public company suspending its operations in Russia and establishing a reserve for outstanding accounts receivable balances of customers in Russia, Belarus, and Ukraine.

The target team observed that engagement teams made changes to their overall audit strategy including:

- Changing planning materiality.
- Reconsidering the legal entities and general ledger accounts that were in scope for the audit.
- Realigning the engagement team's nature, timing, and extent of audit procedures to conform to the audit plan for other locations.
- Removing a Russia component from the group audit scope because the public company paused all shipments to Russia.

In addition, the target team also observed that pre-existing audit firms that were divested from the global network of affiliate audit firms, were being reconstituted as new Russian audit firms.

4. **No Site Visits in Certain Locations** – For five audit firms, and 10 public company audits, the group auditor did not perform site visits at certain locations due to COVID-19 pandemic travel restrictions in China and/or events in Russia and Ukraine. In those instances, the group auditor increased interactions with component teams through remote meetings, video calls, and virtual reviews.

   For one audit firm, and one public company audit, the group auditor performed site visits in Hong Kong as an alternative to visiting mainland China. Specifically, the engagement team traveled to the audit firm's Hong Kong office which had full access to the component team's audit work papers. The engagement team was also able to perform a site visit at the public company's Hong Kong operations.

5. **Resumed Site Visits** – For three audit firms, and four public company audits, the principal auditor resumed in-person site visits with the component teams at locations not deemed to have a safety or security risk at the time of the audit.

6. **Review by U.S. Secondee** – For one audit firm, and one public company audit, the group auditors used U.S. secondees on rotation in China to perform first level reviews of the work papers.

## Good Practices

The following are good practices that may contribute to audit quality in the execution of engagement procedures on multi-location audits:

1. **Engagement Quality Review Procedures over Component Work** – One audit firm required the assignment of an assistant to the engagement quality reviewer to review the work of a component team in a multi-location audit.

2. **Voluntary Consultations** - For two audit firms, and two public company audits, engagement teams completed consultations that were not required by the audit firm related to:

   - Use of an audit firm in Russia, including supervision and review of the component team; and
   - Component scoping decisions.

3. **Voluntary Use of Specialists** – On all audits reviewed at the six audit firms, the group auditor used auditor-employed or auditor-engaged specialists (e.g., valuation, information technology, or forensic) in the planning, scoping, and risk assessment procedures of multi-location audits.

4. **Voluntary Involvement of Fraud Specialists** – For two audit firms and two public company audits, the group auditor voluntarily involved an auditor-employed fraud or forensic specialist to assist with global fraud risk assessments. This assessment included the design and execution of audit procedures of audits with higher engagement risk.

5. **Required Review of Component Auditor Inspections** – For one audit firm and two public company audits, the group auditor required documentation of the results of internal and/or external inspections of the component auditors used. This procedure may heighten the awareness of the group auditor concerning the audit quality of component auditors being contemplated.

6. **Component Auditor's Engagement Letters** – For four audit firms, and six public company audits where the component auditors had separate standalone engagement letters, the group auditor included review of those engagement letters as part of the use of component auditors, although it was not required by the audit firm.

7. **Affirmation of Audit Documentation** – For all public company audits reviewed, the group auditor required component auditors to provide a final set of audit documentation, which included a clearance memo affirming referral instructions were completed via firm-provided practice aids.

## New Requirements for Lead Auditors' Use of Other Auditors

On June 21, 2022, the PCAOB **adopted amendments** to its auditing standards to strengthen requirements that apply to audits involving multiple audit firms and a new auditing standard, AS 1206, *Dividing Responsibility for the Audit with Another Accounting Firm*. These amendments and AS 1206 will take effect for audits of financial statements for fiscal years ending on or after December 15, 2024.

## Significant or Unusual Events or Transactions

The target team performed procedures to review the auditor's efforts regarding the identification and testing of such events or transactions on seven public company audits across five GNF audit firms. The engagement teams evaluated the nature and purpose of potential significant or unusual events or transactions in the context of the public companies' industries and operations on all seven public company audits reviewed. Based on those evaluations, the engagement teams identified three of these events or transactions as significant or unusual. The primary objective of the target team's procedures on such events or transactions was to understand:

1. How did the engagement teams identify and respond to the risk of material misstatement in the financial statements due to error or fraud posed by such events or transactions?

2. Were audit firm personnel with the requisite skills and experience involved in the auditing of such events or transactions?

3. How did audit firm guidance on such events and transactions and the execution of audit procedures vary from audit firm to audit firm?
4. What were the requirements of the audit firm's consultation process for such events and transactions?
5. Were there any communications provided to the audit committee about such events and transactions?
6. Were such events and transactions appropriately identified?

## Observations

The target team noted the following observations:

1. **Identification of Such Events or Transactions** – For two audit firms, and three public company audits, the following such events or transactions were identified:
   - A business acquisition related to the expansion of the public company's market share in the social media and influencer market.
   - A business acquisition broadening the public company's product offerings into new markets; and
   - A goodwill impairment subsequent to the initial accounting for the business combination (i.e., Day 2 accounting considerations) due to a decline in crypto asset prices.
2. **CAMs Identified** – For three audit firms, and three public company audits, CAMs were considered for the following items:
   - Legal contingencies.
   - A restructuring event that resulted in the impairment of intangible assets.
   - Acquisitions; and
   - Cybersecurity events.
3. **No Control Deficiencies and Misstatements** – For all public company audits reviewed, there were no control deficiencies or misstatements related to such events or transactions identified by the engagement team.
4. **Required Consultations** – For one audit firm, and one public company audit, the engagement team consulted with others in the audit firm as required by the audit firm's policies and procedures. The consultation was for matters related to a business acquisition, which was deemed a significant unusual transaction. Specifically, the consultation concerned whether the public company possessed the necessary expertise, including whether it engaged a specialist, and the appropriate audit response, including the involvement of individuals with appropriate expertise.

## Good Practices

The following are good practices that may contribute to audit quality in the execution of the engagement procedures on such events or transactions:

1. **Voluntary Consultations** – For two audit firms, and two public company audits, the engagement teams completed consultations where an audit firm determined consultation was not expressly required. Some examples observed included the accounting for a consumer loan securitization and the novel nature of a "Day 2" goodwill impairment.
2. **Voluntary Use of Specialists** – For four audit firms, and six public company audits, the group auditor involved specialists employed or engaged by the auditor (e.g., valuation specialists) in the planning, scoping, and risk assessment procedures specifically related to such events or transactions.

# 2024 TARGET TEAM INSPECTION ACTIVITIES

During 2024, target team inspection activities will consist of reviewing public company audits focused on the following topics:

- Initial audits by a successor auditor.
- Risk assessment.
- Auditor's assessment of a public company's use of artificial intelligence.
- Biotech startups.
- Audit firms' usage of shared service centers; and
- Cash flow statement, segment reporting, and earnings per share.

Observations from the target team may be shared in future Spotlight documents.

## Tell Us What You Think

Was this Spotlight helpful to you? In fulfilling our mission to serve investors and the public, the PCAOB wants to know how we can improve our communication and provide information that is timely, relevant, and accessible. We welcome comments on this publication or other matters. You can fill out **our short reader survey** or email us at **info@pcaobus.org**.