PCAOB
Public Company Accounting Oversight Board

Audits Involving Cryptoassets

Information for Auditors and Audit Committees

SPOTLIGHT

Overview

One of the PCAOB's strategic objectives is to monitor the development and implementation of emerging technologies to analyze their implications for the quality of audit services.

PCAOB staff has observed that cryptoassets[1] have recently begun to be recorded and disclosed in issuers' financial statements. In addition, when performing inspections of auditors of some smaller issuers, PCAOB staff has observed situations where transactions involving cryptoassets were material to the financial statements.

Observations from these inspections indicate the need for a greater focus by some auditors on the identification and assessment of the risks of material misstatement to the financial statements related to cryptoassets, as well as the planning and performing of an appropriate audit response.

This document highlights considerations for addressing certain responsibilities under PCAOB standards for auditors of issuers transacting in or holding cryptoassets.[2] We also suggest questions that audit committees may consider asking their auditors when transactions involving cryptoassets or holdings of cryptoassets are material to the issuer's financial statements. The information in this Spotlight may be of particular interest to the auditors and audit committee members of issuers that are beginning to transact in, or hold cryptoassets.

This Spotlight does not specifically address any other applications of blockchain, distributed ledger, or other technology.

Contents

The information in this Spotlight is not staff guidance; rather, it highlights timely and relevant observations for auditors and audit committees.

[1] In this publication, the term cryptoasset refers to a digital asset that uses cryptography to secure transactions digitally recorded on a distributed ledger, such as a blockchain. This publication does not specifically address so called "stable coins," which, unlike other types of cryptoassets, purport to use some means to stabilize their price relative to another asset, for example, by reference to a fiat currency.

[2] This document does not specifically highlight considerations for auditors of broker-dealers.

Background

As of the date of this publication, many types of cryptoassets (including Bitcoin, the largest by market value) have been created and are being traded. An issuer's involvement with cryptoassets can be multifaceted. Transactions involving cryptoassets may include, for example, earning a fee, or "reward," for validating new blocks on a blockchain (which for some cryptoassets, such as Bitcoin, is commonly known as "mining"), purchasing goods or services in exchange for cryptoassets, exchanging one cryptoasset for another, or selling cryptoassets for a fiat currency, such as the US dollar. Transactions involving cryptoassets may also include, for example, providing trading services to third parties or acting as an intermediary, such as between a customer and a trading platform or mining operation.

Information for Auditors

Certain Responsibilities under PCAOB Standards

Below we share reminders for auditors about certain areas of responsibility under PCAOB standards at the firm level, relating to the firm's system of quality control, and at the audit engagement level, relating to audit planning and risk assessment.[3] We also provide examples of considerations specific to cryptoassets at the firm level and at the audit engagement level.

At the Firm Level – The Firm's System of Quality Control

Under PCAOB quality control standards, a firm should establish policies and procedures for deciding whether to accept or continue a client relationship and whether to perform a specific engagement for that client. This involves establishing policies and procedures which provide reasonable assurance that:

- ✓ The firm undertakes only those engagements that the firm can reasonably expect to be completed with professional competence. For example:
  - o The performance of audits involving cryptoassets may require certain specialized skill and knowledge, as discussed in more detail below.
  - o The performance of engagement quality reviews would require appropriate level of knowledge and competence relating to cryptoassets.
- ✓ The firm appropriately considers the risks associated with providing professional services in the particular circumstances. For example:
  - o Because holdings of cryptoassets generally are designed to be pseudonymous (i.e., concealing an account holder's real identity behind an alphanumeric code), it may be more difficult for an auditor to recognize when a cryptoassets-related transaction involves fraud or another illegal act, or related parties.

Under PCAOB quality control standards, a firm should establish policies and procedures for deciding whether to accept or continue a client relationship and whether to perform a specific engagement for that client.

[3] For the requirements discussed in this section see generally QC 20, *System of Quality Control for a CPA Firm's Accounting and Auditing Practice*, AS 1220, *Engagement Quality Review*, AS 2101, *Audit Planning*, AS 2110, *Identifying and Assessing Risks of Material Misstatement*, and AS 2301, *The Auditor's Responses to the Risks of Material Misstatement*.

At the Audit Engagement Level – Planning

PCAOB standards on audit planning address, among other things, the engagement team's need for specialized skill or knowledge. In particular:

- ✓ The auditor should determine whether specialized skill or knowledge is needed. For example:
  - o The engagement team may need specialized skill or knowledge in the areas of cryptography, distributed ledger technology, valuation, and laws and regulations (including with respect to know-your-customer (KYC) and anti-money laundering (AML) provisions).
  - o Differing business models and technologies underlying transactions in cryptoassets (e.g., generating new coins vs. trading existing ones) may require different skills, knowledge, and resources (including specialized audit software) to identify, assess, and respond to risks of material misstatement.
  - o The engagement team may need specialized skill or knowledge in applying existing legal and regulatory frameworks to cryptoassets. The U.S. Securities and Exchange Commission (SEC) staff provides information and guidance about digital assets on its website.[4]

At the Audit Engagement Level – Risk Assessment

PCAOB standards on risk assessment address, among other things, identifying and assessing the risks of material misstatement, including obtaining an understanding of the issuer and its environment, and considering the risk of management override of controls.

The auditor should identify and assess the risks of material misstatement to the financial statements, which includes evaluating the types of potential misstatements, assessing the likelihood and magnitude of misstatements, and determining the likely sources of potential misstatements.

The auditor should then design and perform audit procedures in a manner that addresses the assessed risks of material misstatement for each relevant assertion of each significant account and disclosure as applicable (i.e., performing audit procedures that address risks of material misstatement relating to existence or occurrence, completeness, valuation or allocation, rights and obligations, and presentation and disclosure).

- ✓ The auditor should obtain an understanding of the issuer and its environment, which could include obtaining and analyzing relevant information about the nature of the issuer's transactions involving cryptoassets. Such information is key to effective risk identification and assessment and is the basis for planning and performing an appropriate audit response. For example:
  - o The types of potential misstatements associated with balances of cryptoassets could depend on whether the cryptoassets are stored in the issuer's own digital wallet or by a third party.

PCAOB standards on risk assessment address, among other things, identifying and assessing the risks of material misstatement, including obtaining an understanding of the issuer and its environment, and considering the risk of management override of controls.

[4] See, e.g., www.sec.gov/finhub (collecting materials related to digital assets).

- The likelihood and magnitude of potential misstatements associated with transactions involving cryptoassets could depend on the number of cryptoasset types, the number of customers, the volume of transactions, and the nature of recordkeeping (e.g., whether customer transactions are recorded outside the blockchain).
- Determining the likely sources of potential misstatements related to the validating fee could involve considering the structure of the issuer's validating operations, including any involvement of third parties in the provision and pooling of equipment.

✓ The auditor should obtain an understanding of the issuer's objectives, strategies, and related business risks that might reasonably be expected to result in risks of material misstatement. For example:

- The pseudonymous nature of transactions involving cryptoassets may obscure the true identity of the issuer's counterparties, exposing the issuer to the risk of non-compliance with KYC and AML provisions, or the risk of not identifying involvement of related parties.
- The issuer may not have the personnel or expertise to deal with cryptoassets, increasing the risk of error in processing and reporting transactions that involve cryptoassets.

✓ The auditor also should obtain a sufficient understanding of the issuer's internal control over financial reporting, including its information system(s) relevant to financial reporting, to identify the types of potential misstatement, assess the factors that affect the risks of material misstatement, and design further audit procedures.[5] Understanding relevant controls related to transactions involving cryptoassets may include, for example:

- Understanding controls over the generation and management of private keys (i.e., access passcodes), which are important to addressing risks relating to the existence of balances of cryptoassets.
- When important internal controls reside at a third party, determining whether a service auditor's report addresses those controls, or whether the controls would need to be tested directly by the issuer's auditor to obtain evidence of their effectiveness.
- Understanding controls over the reliability of blockchain information to be used as audit evidence (e.g., controls that address alterations to the information stored on blockchain).
- Understanding controls over cryptoasset-related transactions that are recorded outside the blockchain (e.g., information about customer transactions in a trading platform's system) and therefore not covered by the same controls as transactions recorded on the blockchain.

[5] In an integrated audit, the scope of the required understanding of controls may be broader, reflecting the requirement for the auditor to identify and test controls that are important to the auditor's conclusion about whether the issuer's controls sufficiently address the assessed risk of misstatement to each relevant assertion.

- ✓ In identifying fraud risks, the discussion among the key engagement team members about the potential for material misstatement due to fraud may include, for example:
  - o The risk of management override of controls over the private keys, which may result in misuse or misappropriation of holdings of cryptoassets by those who control the keys.
  - o The susceptibility of the financial statements to material misstatement through transactions with related parties. The related parties' identities may be difficult to ascertain because of the pseudonymous nature of transactions involving cryptoassets.

Information for Audit Committees

Questions Audit Committees Could Consider Asking their Auditors

The following sample questions are designed to provide audit committees of issuers that are new to transacting in, or holding cryptoassets, or audit committee members who are new to cryptoassets, with ideas of the types of questions they may consider—at their discretion—asking their auditors.

- ✓ What is the experience of the engagement partner and other senior engagement team members with cryptoassets? Would the firm be able to supplement the engagement team's expertise if necessary (e.g., by engaging relevant specialists)?
- ✓ What is the auditor's understanding of the technology underlying the issuer's cryptoasset-related activities?
- ✓ Are specialized technology-based audit tools needed to identify, assess, and respond to risks of material misstatement?
- ✓ What is the auditor's understanding of the legal and regulatory (including KYC and AML) implications of the issuer's cryptoasset-related activities?
- ✓ How does the audit firm monitor auditor independence considerations associated with audit engagements involving cryptoassets (e.g., monitoring whether its staff invests in cryptoassets)?
- ✓ What policies and procedures does the audit firm have regarding conducting and monitoring audit engagements involving cryptoassets, including considering the risks associated with performing such audits?

What's Next?

The Board is committed to understanding the impact of emerging technologies, including cryptoassets, on audit firms, issuers, audit committees, and investors as it relates to the audits of issuers and brokers-dealers. PCAOB staff will continue to monitor technology-related developments and assess their implications for PCAOB standards.

Other Resources

The Canadian Public Accountability Board discusses findings from its inspections of audits involving cryptoassets. See *Auditing in the Crypto-Asset Sector Inspections Insights*. (Accessed on May 19, 2020. The PCAOB is not endorsing this publication, but is providing the reference for information only.)

We Want to Hear from You

In an effort to continue to improve external communications and provide information that is timely, relevant, and accessible, we want to hear your views regarding this document. **Please take 2 minutes to fill out our short survey.**

Stay Connected to PCAOB

Contact Us | Subscribe | PCAOB | @PCAOB_News