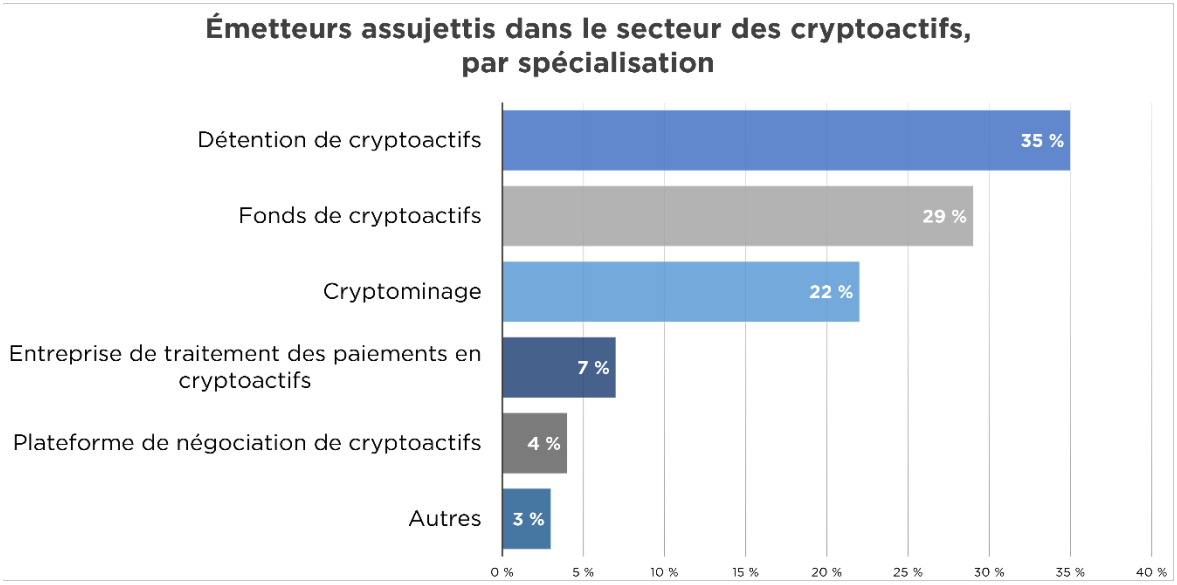
L'échange ccrc

Points de vue sur les inspections des cryptoactifs

Le contexte dans lequel les émetteurs assujettis exercent leurs activités dans le domaine des cryptoactifs[1] continue d'évoluer. Le Conseil canadien sur la reddition de comptes (CCRC) reconnaît que cette évolution crée des défis tant pour les émetteurs assujettis que pour les cabinets d'audit du secteur. La présente publication donne un aperçu et des exemples illustratifs de constatations courantes d'inspection pour les auditeurs d'émetteurs assujettis de cryptoactifs. Elle souligne également les bonnes pratiques observées dans les dossiers d'audit sans constatation et met en évidence certains risques émergents.

En février 2024, on comptait 72 émetteurs assujettis canadiens dans le secteur des cryptoactifs, audités par 26 cabinets comptables inscrits auprès du CCRC. Le tableau ci-dessous indique le principal domaine de spécialisation dans lequel ces émetteurs assujettis exercent leurs activités.



Ce que révèlent nos inspections

Entre 2020 et 2023, le CCRC a inspecté 33 dossiers d'audit d'émetteurs assujettis exerçant des activités liées aux cryptoactifs et a relevé des constatations importantes[2] dans 23 de ces dossiers. Bien que nous ayons constaté des améliorations dans les procédures mises en œuvre par les auditeurs des émetteurs assujettis dans ce secteur, une tendance à la baisse du taux de constatations (en 2020, tous les dossiers inspectés comportaient des

[1] Le terme « cryptoactif » désigne généralement les actifs numériques tels que les cryptomonnaies, les jetons, etc., qui utilisent la cryptographie et le dispositif d'enregistrement électronique partagé pour créer, vérifier et sécuriser les transactions.
[2] Une constatation importante découlant de l'inspection se définit comme une déficience importante dans l'application des normes d'audit généralement reconnues à un ensemble important d'opérations ou à un solde financier important, le cabinet d'audit devant alors réaliser des travaux d'audit supplémentaires pour étayer son opinion ou apporter des modifications importantes à sa stratégie d'audit.

constatations importantes par rapport à 50 % en 2023), les types de constatations d'inspection et le taux de constatations demeurent inacceptablement élevés.

La présente publication fait état de certains risques émergents dans le secteur des cryptoactifs. Les enjeux et les risques mentionnés dans celle-ci ne doivent pas être considérés comme une liste exhaustive. Il incombe à l'auditeur de déterminer les procédures d'audit appropriées, conformément aux normes d'audit applicables, en fonction des faits et circonstances propres à l'émetteur assujetti.

Constatations d'inspection importantes courantes

Aucune détermination ou prise en compte des risques particuliers associés aux cryptoactifs n'a été effectuée, dont les risques de fraude.

Parmi les 23 dossiers ayant fait l'objet de constatations d'inspection importantes, 8 ont révélé que l'auditeur ne possédait pas une connaissance suffisante des risques opérationnels particuliers associés aux émetteurs assujettis de cryptoactifs. Ce niveau de constatations indique que les auditeurs doivent en faire davantage pour s'assurer qu'ils acquièrent une bonne connaissance de l'entité et qu'ils détiennent la connaissance spécialisée du secteur qui leur permettra d'identifier et d'évaluer efficacement les risques d'anomalies significatives.

Voici des exemples de constatations découlant de nos inspections :

- L'auditeur n'avait pas identifié ou évalué convenablement un risque important lié à l'existence et à la propriété des cryptoactifs.
- L'auditeur n'avait pas acquis la connaissance de la logique opérationnelle d'une transaction de cryptoactifs.
- L'auditeur n'avait pas tenu compte des risques de fraude associés à des transactions de cryptoactifs particulières impliquant des apparentés.

Les auditeurs doivent s'assurer qu'ils comprennent les risques particuliers liés aux activités de l'émetteur assujetti, les relations et transactions avec les apparentés, ainsi que l'intégrité et la compétence

Le risque de fraude pour toutes les transactions de cryptoactifs est élevé en raison de la nature des opérations et du pseudo-anonymat des parties impliquées. Voici quelques exemples de risques de fraude à prendre en compte par les auditeurs des émetteurs assujettis de cryptoactifs :

- Les clés privées utilisées pour accéder aux cryptoactifs ne sont pas protégées de manière appropriée pour éviter leur vol ou leur corruption.
- La protection des droits de propriété des cryptoactifs contre l'interception ou la revendication par des personnes non autorisées nécessite une technologie sophistiquée et de rigoureux protocoles de cybersécurité. Si ceux-ci ne sont pas établis, les cryptoactifs sont susceptibles de faire l'objet d'une utilisation et d'un accès frauduleux ou d'un transfert à des cybercriminels.
- Les transactions inhabituelles ou complexes concernant des cryptoactifs sans justification opérationnelle manifeste peuvent indiquer que la transaction est motivée par une autre finalité, en particulier lorsqu'il s'agit d'une transaction entre apparentés.

globales de la direction[3]. Les auditeurs doivent se demander si la gouvernance de l'émetteur assujetti de cryptoactifs est limitée ou inexistante et déterminer l'incidence que cela peut avoir sur l'évaluation globale des risques[4]. Enfin, les auditeurs doivent également comprendre l'environnement juridique et réglementaire des cryptoactifs, y compris les exigences précises en vigueur dans les différentes juridictions[5].

> Les scénarios présentés dans la présente publication sont représentatifs des types de problèmes relevés lors de nos inspections. Les faits ont été modifiés ou exclus afin de protéger l'identité des émetteurs assujettis.

Exemple: Achat d'équipement à un apparenté au moyen de cryptoactifs

Contexte

Une entité exerçant des activités liées aux cryptoactifs avait acheté de l'équipement à un apparenté. L'entité avait payé l'équipement au moyen de cryptoactifs qui avaient été transférés à l'apparenté par l'intermédiaire d'une plateforme de négociation de cryptoactifs gérée par le même apparenté.

Approche d'audit

L'équipe de mission n'avait pas identifié de risque important ou de fraude lié à cette transaction. Elle avait conclu que les procédures de corroboration permettaient d'obtenir des éléments probants suffisants et appropriés pour valider l'existence, la propriété et l'évaluation de l'équipement, et avait examiné les factures préparées par l'apparenté pour en valider l'achat. L'équipe de mission avait également approuvé le paiement et le transfert des cryptoactifs en confirmant les montants payés (c.-à-d. les cryptoactifs) dans un rapport d'activité de la plateforme de négociation de cryptoactifs.

Constatations

L'équipe de mission n'avait pas évalué s'il existait une justification opérationnelle raisonnable pour la transaction ni examiné si celle-ci avait été conclue dans le but de produire de l'information financière frauduleuse ou de camoufler une mauvaise affectation des actifs[6]. L'évaluation des risques n'avait pas été effectuée de manière adéquate, car l'équipe de mission n'avait pas identifié le risque d'anomalies significatives pouvant exister lors de l'achat d'actifs auprès d'un apparenté. Les risques particuliers au niveau des assertions relatives à l'existence, la propriété et l'évaluation des actifs n'avaient pas été évalués de manière appropriée. Par exemple, l'équipe de mission n'avait pas examiné si le montant payé pour l'équipement acquis et les cryptoactifs transférés reflétaient la juste valeur de la transaction. Par conséquent, les éléments probants obtenus n'étaient pas suffisants pour répondre aux risques d'anomalies significatives associés à la transaction.

[3] NCA 315, alinéa 19a).
[4] NCA 315, sous-alinéa 19a)(i).
[5] NCA 315, sous-alinéa 19a)(ii).
[6] NCA 240, alinéa 33c).

En mars 2024, le CCRC a publié le rapport intitulé Identification et évaluation des risques d'anomalies significatives : renforcer la qualité de l'audit, qui fournit des renseignements supplémentaires sur l'identification et l'évaluation des risques d'anomalies significatives.

Compréhension insuffisante du système de contrôles internes de l'entité et réponse inappropriée à l'évaluation des risques.

L'environnement numérique dans lequel les cryptoactifs sont détenus et échangés dépend fortement des systèmes et des applications des technologies de l'information (TI). Dans 15 des 23 dossiers ayant fait l'objet de constatations d'inspection importantes, nous avons observé un manque de compréhension des processus et, souvent, une absence d'évaluation du système de contrôles internes de l'entité. Ces observations ont donné lieu à des constatations importantes, car rien n'indiquait que l'auditeur avait déterminé si des procédures de corroboration pouvaient à elles seules fournir suffisamment d'éléments probants au regard des risques d'inexactitudes importantes au niveau des assertions[7].

Voici des exemples de constatations découlant de nos inspections :

- L'auditeur avait conçu une approche d'audit de corroboration pour un émetteur assujetti de cryptoactifs dont le soutien de l'audit reposait sur des données et des rapports (c.-à-d. des registres détaillés des transactions de cryptoactifs de l'émetteur assujetti) provenant d'un système TI développé à l'interne. Toutefois, aucune procédure d'audit n'avait été effectuée pour vérifier l'exhaustivité et l'exactitude des renseignements contenus dans le système TI développé à l'interne.

- Les procédures de corroboration effectuées par l'auditeur dépendaient de la conception et mise en œuvre efficaces des contrôles internes sur la protection des clés privées. Cependant, aucune procédure d'audit n'avait été effectuée sur les contrôles internes pour s'en assurer.

- L'auditeur avait identifié des lacunes de contrôles liées au traitement et à l'enregistrement des transactions de cryptoactifs, mais il n'avait pas tenu compte de l'incidence de ces lacunes sur la conception et la mise en œuvre d'autres procédures d'audit. De plus, l'auditeur n'avait pas communiqué de manière appropriée les lacunes de contrôles aux responsables de la gouvernance.

Même si l'auditeur ne prévoit pas s'appuyer sur les contrôles internes dans le cadre de sa stratégie d'audit, il doit acquérir une connaissance de l'environnement de contrôle pertinent pour la préparation des états financiers, qui peut inclure les contrôles généraux des technologies de l'information et d'autres contrôles informatiques[8]. Les auditeurs peuvent juger utile d'acquérir cette connaissance dans le cadre du processus d'acceptation et de maintien de relations clients.

[7] NCA 315, paragraphe 33.

[8] NCA 315, paragraphe 21.

Exemple : Comptabilisation des revenus par une entreprise de traitement des paiements en cryptoactifs

Contexte

Un émetteur assujetti qui se spécialise dans le traitement des paiements en cryptoactifs facilite les transactions entre les commerçants qui vendent des biens et les clients qui utilisent des cryptoactifs comme mode de paiement. Les commerçants reçoivent leurs dus dans une monnaie fiduciaire sous-jacente (c.-à-d. en espèces). L'émetteur assujetti facture des frais de service fondés sur un pourcentage de la transaction de cryptoactifs. Le système de traitement des paiements de cryptoactifs est hautement automatisé et facilite un grand volume de transactions quotidiennes avec peu ou pas d'intervention manuelle.

Approche d'audit

L'équipe de mission avait adopté une approche de corroboration pour tester l'exactitude et la réalité des revenus gagnés. Les principaux éléments probants obtenus comprenaient le recoupement des encaissements versés aux commerçants avec un rapport généré par le système qui justifie le montant des revenus comptabilisés.

Constatations

L'équipe de mission n'avait pas obtenu suffisamment d'éléments probants appropriés pour remédier aux risques d'inexactitudes importantes liées à l'exhaustivité, à l'exactitude et à la réalité des revenus. Aucune évaluation de la conception et de la mise en œuvre des contrôles internes (y compris les contrôles informatiques) relatifs au système de traitement des paiements n'avait été réalisée et, par conséquent, les procédures de corroboration n'avaient pas fait l'objet d'un examen visant à déterminer si elles étaient suffisantes à elles seules pour répondre aux risques d'anomalies significatives. Les procédures d'audit reposaient implicitement sur l'efficacité des contrôles du système de traitement des paiements, notamment sur le calcul des droits gagnés et sur la conversion des cryptoactifs en espèces.

Jalonnement de cryptoactifs

Certains émetteurs assujettis se sont livrés au jalonnement de cryptoactifs pour obtenir un rendement sur leurs cryptoactifs. En raison de la rapidité et de l'efficacité énergétique, le modèle basé sur la validation du jalon s'impose comme le mécanisme privilégié pour valider et sécuriser les transactions sur une chaîne de blocs. En ce qui concerne les cryptoactifs jalonnés, les risques liés au processus de validation peuvent différer selon que la validation soit effectuée par l'émetteur assujetti (valideur) ou que l'émetteur assujetti confie la validation à un tiers (délégant).

Lorsque l'émetteur assujetti est le valideur[9], les auditeurs devraient pouvoir tenir compte des contrôles internes pertinents sur les systèmes TI de l'entité utilisés pour valider les transactions et déterminer si leur efficacité opérationnelle devrait être testée. Lorsque l'émetteur assujetti est un délégant[10], les auditeurs devraient tenir compte de la fiabilité des renseignements reçus de la société de services responsable de la validation des transactions (y compris les facteurs à considérer mentionnés dans la section ci-dessous). Dans certains cas, les

[9] Un valideur est un participant à la chaîne de blocs qui vérifie les transactions sur une chaîne de blocs à preuve d'enjeu dans le cadre de son mécanisme de consensus. Les valideurs exploitent un nœud pour signer les transactions de la chaîne de blocs comme étant valides.

[10] Un délégant est une personne ou une entité qui confie ses cryptoactifs à un valideur de confiance au lieu d'exploiter un nœud et de valider lui-même les transactions de la chaîne de blocs.

cryptoactifs jalonnés peuvent être bloqués pendant une période déterminée. Cette restriction doit être prise en compte dans le cadre de l'évaluation par l'auditeur de l'évaluation des cryptoactifs jalonnés. Les auditeurs devraient également s'interroger sur les procédures à mettre en œuvre pour répondre aux risques liés à la comptabilisation des avantages tirés des actifs jalonnés, y compris le risque présumé de fraude lors de la comptabilisation des revenus.

Aucune évaluation de la fiabilité des renseignements fournis par des tiers n'a été réalisée.

Dans 13 des 23 dossiers faisant l'objet de constatations importantes, le CCRC a constaté que les auditeurs n'avaient pas évalué la fiabilité des renseignements obtenus auprès de tiers ou des outils de tiers utilisés pour recueillir des éléments probants[11].

Voici des exemples de constatations découlant de nos inspections :

- L'auditeur n'avait pas recueilli suffisamment d'éléments probants appropriés pour étayer la pertinence et la fiabilité des renseignements fournis par des tiers (p. ex. les dépositaires et échanges de cryptoactifs) pour corroborer l'existence ou la propriété des cryptoactifs détenus auprès de ces tiers. Dans les cas où un rapport de contrôle de la société de services était disponible, l'auditeur n'avait pas pris en considération la fiabilité de ce rapport et les contrôles complémentaires pertinents de l'utilisateur final requis pour s'appuyer sur la société de services[12]. Lorsqu'un rapport de contrôle de la société de services n'était pas disponible, l'auditeur n'avait pas examiné s'il aurait été pertinent d'acquérir une connaissance de l'environnement de contrôle ou d'évaluer la conception, la mise en œuvre et l'efficacité opérationnelle des contrôles pertinents auprès des tiers détenant les cryptoactifs[13].

- L'auditeur s'était appuyé sur l'utilisation d'outils de tiers, tels que des explorateurs de chaîne de blocs publics, pour obtenir des renseignements qui étaient enregistrés dans des grands livres distribués, sans valider la fiabilité et la pertinence de l'outil.

- Les confirmations de tiers avaient été obtenues comme principale source d'éléments probants attestant que l'émetteur assujetti avait des droits légitimes sur les cryptoactifs détenus par des tiers. Cependant, aucune évaluation de la fiabilité des renseignements inclus dans la réponse à la demande de confirmation n'avait été réalisée[14]. Ce faisant, l'auditeur s'était implicitement appuyé sur l'efficacité opérationnelle des contrôles internes du tiers sans procéder à une évaluation ou à des tests supplémentaires.

Pour obtenir des renseignements supplémentaires au sujet des sociétés de services, veuillez consulter la publication du CCRC sur les facteurs à considérer pour l'audit d'entités faisant appel à une société de services.

[11] NCA 500, paragraphe 7; NCA 402, paragraphe A26.
[12] NCA 402, paragraphe 17.
[13] NCA 402, alinéa 16b).
[14] NCA 402, alinéa A26c).

Exemple : Cryptoactifs détenus par un tiers

Contexte

Un émetteur assujetti détient des cryptoactifs et effectue des transactions avec ceux-ci. Il fait appel à un tiers dépositaire pour sécuriser ses cryptoactifs.

Approche d'audit

L'équipe de mission avait acquis une compréhension des services fournis par le tiers dépositaire en s'informant auprès de la direction. La principale source d'éléments probants était la confirmation du tiers dépositaire, qui a fourni l'historique des transactions effectuées au cours de la période visée et les cryptoactifs détenus à la fin de l'exercice de l'émetteur assujetti.

Constatations

Les procédures mises en œuvre étaient insuffisantes, car la compréhension de l'auditeur s'était limitée à des demandes de renseignements, et l'équipe de mission n'avait pas évalué de manière appropriée la fiabilité des renseignements fournis dans la confirmation reçue par le tiers dépositaire. Aucune procédure n'a été mise en œuvre pour mieux comprendre les services fournis par le tiers dépositaire. L'équipe de mission n'avait pas évalué s'il s'agissait d'une société de services et n'avait pas non plus compris les risques associés à l'utilisation des renseignements fournis par le tiers dépositaire. Par exemple, l'auditeur n'avait pas examiné si les cryptoactifs détenus par le tiers étaient regroupés parmi d'autres ou s'il existait des contrôles appropriés et efficaces sur la protection des cryptoactifs détenus par le tiers.

Utilisation et fiabilité des contrats intelligents

Les contrats intelligents au sein des plateformes de financement décentralisées sont des contrats auto-exécutoires dont les modalités de l'entente entre les parties sont directement inscrites dans le code. Les contrats intelligents peuvent être sujets à des erreurs de codage et, s'ils ne sont pas correctement codés, ils sont vulnérables à l'exploitation. Cette vulnérabilité est attribuable à l'immuabilité de la chaîne de blocs une fois que le contrat intelligent est déployé. Les transactions qui s'appuient sur des contrats intelligents peuvent être vulnérables aux divergences de code et au piratage.

La direction peut remettre aux auditeurs un audit[15] de contrat intelligent à titre d'élément probant. Les audits de contrats intelligents examinent habituellement le fonctionnement et le code d'un contrat intelligent et peuvent contribuer à détecter des vulnérabilités dans le code ou le déploiement du contrat grâce à l'examen du code, aux tests de pénétration et aux tests de fonctionnalité. Ils peuvent être utilisés par la direction pour démontrer que le contrat intelligent fonctionne comme prévu.

Il est important de prendre note que, bien qu'un audit de contrat intelligent puisse être désigné comme un « audit », il peut ne pas être préparé conformément aux normes d'assurance[16], et les auditeurs doivent être conscients de cette limitation s'ils l'utilisent comme élément probant. À l'instar des rapports de « preuve de réserve » publiés par certaines plateformes d'échange ou bourses de cryptomonnaies, les audits de contrats

[15] Le terme « audit » est habituellement associé aux audits d'états financiers historiques, mais il est ici utilisé pour décrire une « autre forme d'assurance ». Ces audits ne sont pas réalisés conformément aux normes canadiennes d'audit (NCA).
[16] Comme les Normes canadiennes de missions de certification (NCMC).

intelligents ne fournissent pas toujours l'information nécessaire aux auditeurs pour étayer leur opinion d'audit. Par exemple, il s'agit généralement de missions ponctuelles qui n'abordent pas les contrôles internes.

Les travaux d'audit effectués pour évaluer les transactions et les événements complexes liés aux cryptoactifs sont insuffisants.

L'évolution de l'utilisation des cryptoactifs donne souvent lieu à des transactions nouvelles, inhabituelles et complexes qui nécessitent une part importante de jugement professionnel. Les auditeurs doivent s'assurer que suffisamment d'éléments probants appropriés sont recueillis[17] pour appuyer la comptabilisation des transactions et des soldes, ainsi que les divulgations relatives aux modèles d'affaires, aux opérations et au rendement. Dans 6 des 23 dossiers ayant fait l'objet de constatations d'inspection importantes, le CCRC a observé un manque d'éléments probants pour étayer les conclusions de l'auditeur quant à la comptabilisation par la direction d'opérations et d'événements complexes.

Voici des exemples de constatations découlant de nos inspections :

- L'auditeur n'avait pas acquis une connaissance suffisante du raisonnement opérationnel ou de la substance économique de la transaction de cryptoactifs. Par exemple, lors de l'évaluation des obligations de performance[18], les éléments probants recueillis pour évaluer les promesses implicites et explicites entre l'émetteur assujetti de cryptoactifs et le client étaient limités, voire inexistants. Cette situation s'était traduite par une comptabilisation inappropriée et non étayée de la transaction.

- Les interrelations entre toutes les parties impliquées dans la transaction de cryptoactifs n'avaient pas été analysées, de sorte que certaines relations entre apparentés n'avaient pas été identifiées ou n'avaient pas fait l'objet d'une divulgation appropriée dans les états financiers[19].

- L'auditeur n'avait pas tenu compte de manière appropriée des éléments probants contradictoires ni appliqué un niveau approprié de scepticisme professionnel pour remettre en cause la position comptable adoptée par la direction[20]. Par exemple, la direction avait évalué la vente d'un jeton numérique comme étant une vente de produit ponctuelle. L'auditeur avait approuvé le traitement comptable retenu par la direction sans prendre en considération d'autres éléments probants qu'il avait recueillis et qui indiquaient que les jetons numériques avaient été vendus dans le cadre d'un contrat de licence. Par conséquent, l'auditeur n'avait pas suffisamment remis en cause le calendrier de comptabilisation des revenus malgré des éléments probants contradictoires.

Les auditeurs devraient se demander si une consultation officielle avec des experts spécialisés[21], notamment des spécialistes des cryptomonnaies, est nécessaire pour s'assurer que les conclusions de la direction sont raisonnables et conformes aux directives comptables pertinentes.

[17] NCA 500, paragraphe 6.
[18] IFRS 15, paragraphe 24.
[19] NCA 550, paragraphes 3 et 4.
[20] NCA 550, paragraphes 3 et 4.
[21] NCA 550, paragraphes 3 et 4.

Exemple : Acquisition d'une société de technologie de chaîne de blocs

Contexte

Un émetteur assujetti a acquis une société de cryptoactifs. Cette dernière développait une plateforme de négociation de cryptoactifs et des cryptoactifs exclusifs qui pouvaient être utilisés sur sa plateforme de négociation. Les cryptoactifs n'ont pas été comptabilisés comme des actifs identifiables inclus dans la répartition du prix d'achat (PPA) pour le regroupement d'entreprises. Les revenus tirés de la vente des cryptoactifs avant et après la date d'acquisition ont été constatés à titre de revenus par l'émetteur assujetti.

Approche d'audit

L'équipe de mission avait obtenu l'évaluation du regroupement d'entreprises par la direction et le rapport d'évaluation de l'expert de la direction comme éléments probants de l'acquisition. L'équipe de mission avait inclus dans son dossier d'audit la politique de comptabilisation des revenus de la direction afin d'étayer le calendrier de comptabilisation.

Constatations

L'équipe de mission n'avait pas suffisamment évalué la complexité de la transaction pour s'assurer que les conclusions comptables déterminées par la direction étaient appropriées. Plus précisément :

- L'équipe de mission n'avait pas remis en question les conclusions de la direction ni évalué de manière appropriée les raisons pour lesquelles les cryptoactifs n'avaient pas été comptabilisés à titre d'actifs identifiables dans la répartition du prix d'achat pour le regroupement d'entreprises.
- L'équipe de mission n'avait pas évalué de manière appropriée les renseignements contradictoires relatifs à la vente des cryptoactifs.
- Les éléments probants recueillis étaient insuffisants pour appuyer les conclusions de l'équipe de mission quant à la pertinence de la politique de constatation des revenus adoptée par la direction.

Emprunt et prêt de cryptoactifs

Les ententes d'emprunt et de prêt de cryptoactifs impliquent souvent des complexités particulières et différentes qui exigent un jugement important et un examen minutieux des faits et des circonstances. Les auditeurs devraient acquérir une compréhension suffisante des modalités de l'entente d'emprunt ou de prêt. L'auditeur peut également envisager d'obtenir un avis juridique pour s'assurer que tous les éléments du contrat ont été évalués adéquatement.

Bonnes pratiques observées dans les dossiers ne faisant l'objet d'aucune constatation

Nous avons constaté des progrès réalisés dans les procédures d'audit conçues et mises en œuvre pour répondre à certains risques et assertions. Les dossiers d'audit qui n'ont pas fait l'objet de constatations importantes regroupent une équipe de mission avec une expertise et des connaissances suffisantes ou impliquent des spécialistes en la matière lors des étapes de planification et d'exécution de l'audit.

Voici des exemples de procédures d'audit observées lors d'inspections d'auditeurs d'émetteurs assujettis de cryptoactifs n'ayant pas donné lieu à des constatations importantes :

- L'auditeur avait mis en œuvre des procédures précises d'évaluation des risques afin d'identifier les risques particuliers d'inexactitudes importantes. Par exemple, il avait procédé à une évaluation détaillée des facteurs de risque de fraude et des risques technologiques connexes propres aux faits et circonstances des transactions et activités sous-jacentes de cryptoactifs de l'émetteur assujetti.

- L'auditeur avait documenté une description détaillée des processus et avait effectué des procédures pas-à-pas pour les flux de transactions de cryptoactifs qui démontraient une compréhension et une identification des contrôles internes pertinents et/ou des lacunes en matière de contrôles. De plus, l'auditeur avait évalué la conception et la mise en œuvre des contrôles internes pertinents, y compris les contrôles généraux et d'applications TI et, lorsque nécessaire, avait testé leur efficacité opérationnelle. Lorsque des lacunes en matière de contrôles avaient été relevées, les auditeurs déterminaient si des contrôles compensatoires existaient et fonctionnaient efficacement ou si des procédures d'audit supplémentaires s'avéraient nécessaires. Toutes les lacunes en matière de contrôles relevées avaient également été communiquées de manière appropriée aux responsables de la gouvernance.

- L'auditeur avait impliqué et consulté des spécialistes au cours du processus d'évaluation des risques et de la conception des procédures d'audit (p. ex. des experts en TI et en chaîne de blocs).

- L'interaction entre la société de services tierce et l'émetteur assujetti, y compris le flux d'information et le degré de dépendance à l'égard de la société de services, était clairement comprise et évaluée par l'auditeur afin de s'assurer que des procédures d'audit appropriées étaient conçues et mises en œuvre.

- L'auditeur avait évalué si les éléments probants recueillis auprès de tiers, tels que les dépositaires ou les bourses de cryptoactifs, étaient suffisamment pertinents et fiables, ou si des éléments probants supplémentaires s'avéraient nécessaires.

- Il y avait suffisamment d'éléments probants appropriés pour remettre en question les conclusions comptables de la direction ainsi que les éléments probants corroborants et contradictoires.

- L'auditeur avait évalué l'environnement législatif et réglementaire dans toutes les juridictions où l'entité exerce ses activités, y compris à l'extérieur du Canada. Il avait fait appel à un expert du secteur pour l'aider à identifier les cas de non-conformité et avait obtenu un avis juridique externe.

Pour en savoir plus

Le CCRC continue de surveiller les enjeux émergents dans le secteur des cryptoactifs au moyen de ses inspections et de faire part de ses observations par l'entremise de divers moyens de communication. Pour en savoir plus sur les précédents points de vue sur l'audit du CCRC dans le secteur des cryptoactifs, veuillez consulter notre site Web.

Consultez notre site Internet au https://cpab-ccrc.ca/fr/acceuil et inscrivez-vous à notre liste de diffusion. Suivez-nous sur LinkedIn.

www.cpab-ccrc.ca / Courriel: info@cpab-ccrc.ca

cpab ccrc Canadian Public Accountability Board Conseil canadien sur la reddition de comptes