



# حسابداری و حسابرسی

## دارایی های دیجیتالی

بخش دوم: حسابرسی

برگردان به فارسی:

مرتضی اسدی الهام ثمری خلج



## قابل توجه خوانندگان

هدف این رهنمود عملی، ارائه راهنمایی غیر رسمی در مورد نحوه حسابداری و حسابرسی دارایی‌های دیجیتالی به ترتیب تحت اصول حسابداری پذیرفته شده ایالات متحده (GAAP) برای نهادهای غیر دولتی و استانداردهای عمومی پذیرفته شده حسابرسی (GAAS) است. این راهنما برای تهیه‌کنندگان و حسابرسان صورت‌های مالی با دانش زمینه‌ای از فناوری بلاکچین در نظر گرفته شده است. برای اهداف این رهنمود عملی، دارایی‌های دیجیتالی به طور کلی به عنوان سوابق دیجیتالی تعریف می‌شوند که با استفاده از رمزنگاری برای تایید و اهداف امنیتی، بر روی یک دفترکل توزیع شده (که به عنوان بلاکچین شناخته می‌شود) ایجاد می‌شوند. دفترکل توزیع شده کلیه معاملات در شبکه بلاکچین را ثبت می‌کند. دارایی‌های دیجیتالی، همانطور که در اینجا تعریف شده است، ممکن است با قابلیت خود برای مقاصد مختلفی از جمله به عنوان یک وسیله مبادله، نماینده ارائه یا دسترسی به کالاها یا خدمات، یا به عنوان یک ابزار تامین مالی، مانند اوراق بهادار، در میان کاربردهای دیگر، مشخص شود. حقوق و تعهدات مربوط به دارایی‌های دیجیتال به طور قابل توجهی متفاوت است، همان‌طور که اصطلاحات مورد استفاده برای توصیف آن‌ها بکار برده می‌شود. توجه به این نکته حائز اهمیت است که نحوه حسابداری برای یک دارایی دیجیتالی در نهایت باتوجه به شرایط خاص، شکل، حقوق اساسی و تعهدات دارایی دیجیتال انجام می‌شود.

دارایی‌های دیجیتالی و فناوری زیربنایی مرتبط با آن، یک حوزه در حال تحول است و انتظارات و تجارب ذینفعان مانند تهیه‌کنندگان، حسابرسان و قانون‌گذاران ممکن است به همین ترتیب تغییر کند. بنابراین سوالات، نمونه‌ها، چالش‌ها، مخاطرات، ملاحظات و رویه‌های احتمالی ذکر شده در این رهنمود عملی نباید جامع تلقی شوند. تهیه‌کنندگان، حسابرسان و ارکان راهبری باید در جریان پیشرفت‌ها قرار گرفته و پیامدهای این تحولات را در نظر بگیرند.

راهنمایی در این رهنمود عملی براساس ادبیات حرفه‌ای موجود و تجربه اعضای کارگروه دارایی‌های دیجیتالی است. این راهنمای غیر رسمی نشان‌دهنده نظرات کارگروه دارایی‌های دیجیتالی و کارکنان انجمن حسابداران رسمی آمریکا (AICPA) است. این نشریه توسط هیئت تدوین استانداردهای حسابرسی، اعضا یا ارکان راهبری انجمن حسابداران رسمی آمریکا تایید، رد یا بکار گرفته نشده است و جزء بیانیه‌های رسمی انجمن حسابداران رسمی آمریکا نیست.

# بخش دوم: حسابرسی

## محتوای حسابرسی

این اطلاعات نشان دهنده نظرات کارکنان انجمن حسابداران رسمی آمریکا بر اساس اطلاعات دریافتی از کارگروه دارایی‌های دیجیتالی است و توسط کمیته ارشد انجمن حسابداران رسمی آمریکا تایید نشده است. بخش حسابرسی این رهنمود عملی، سایر نشریه‌های حسابرسی است که در بخش AU-C200، اهداف کلی حسابرس مستقل و نحوه انجام حسابرسی مطابق با استانداردهای عمومی پذیرفته شده حسابرسی، تعریف شده است و هدف آن ارائه راهنمایی غیر رسمی برای حسابسان است. سایر نشریه‌های حسابرسی ممکن است به حسابرس کمک کند تا استانداردهای عمومی پذیرفته شده حسابرسی را بفهمد و از آن استفاده کند اما حالت الزامی ندارد. در استفاده از رهنمودهای حسابرسی که در سایر نشریه‌های حسابرسی آمده، حسابرس باید از قضاوت حرفه‌ای استفاده کند و ارتباط و مناسب بودن چنین رهنمودهایی را با شرایط حسابرسی ارزیابی کند.

## فهرست

پذیرش و ادامه کار صاحبکار [منتشر شده در جولای ۲۰۲۰]

---

۱	بررسی اجمالی	۵
۲	مجموعه مهارت‌ها و صلاحیت‌های حسابرس	۶
۳	مجموعه مهارت‌های مدیریت و صلاحیت‌ها	۱۴
۴	صلاحیت اخلاقی مدیریت و استراتژی کلی کسب و کار	۱۸
۵	فرآیندها، کنترل‌ها، از جمله فناوری اطلاعات	۲۶

## زیر گروه حسابرسی

### پذیرش و ادامه کار با صاحبکار

#### بررسی اجمالی

مباحث موجود در این بخش از رهنمود عملی، مباحثی است که حسابرسان در مورد پذیرش یا ادامه کار حسابرسی واحدهای تجاری درون اکوسیستم دارایی‌های دیجیتالی جاری، در نظر می‌گیرند. از آنجا که شرکت‌ها به دنبال حسابرسی واحدهای تجاری درون اکوسیستم هستند، باید احتیاط و توجه به ریسک‌ها و چالش‌های منحصر به فرد در اکوسیستم دارایی‌های دیجیتال انجام شود.

مباحث این بخش از رهنمود عملی بر برنامه‌های حسابرسی متمرکز است و آیین اخلاقی یا ملاحظات مربوط به استقلال را بیان نمی‌کند. توجه به این نکته مهم است که اگر چه این ملاحظات برای انطباق حسابرس با استانداردهای حرفه‌ای، بااهمیت باقی می‌ماند اما کار حسابرسی در اکوسیستم دارایی دیجیتال ممکن است ریسک تطبیق جدید یا متفاوتی را ایجاد کند که مستلزم بررسی بیشتر توسط حسابرس است. به عنوان مثال، یک عضو تیم حسابرسی ممکن است دارایی‌های دیجیتالی صادر شده توسط واحد تجاری مورد حسابرسی را نگهداری کند. بخش ET ۱,۲۰۰، "استقلال"، مثالهایی از روابط یا شرایطی را فراهم می‌کند که مخاطراتی را برای رعایت "قواعد استقلال" ایجاد می‌کند و بخش ET ۱,۲۹۵، "خدمات غیراعباردهی"، مخاطرات مربوط به ارائه خدمات غیراعبار-دهی به صاحبکار حسابرسی، از جمله موارد زیر را به طور خاص در نظر می‌گیرد:

- ♦ **خطر خود بینی در تجدید نظر** - خطر اینکه عضو تیم حسابرسی نتایج قضاوت قبلی یا خدمتی که عضو (یا همکار) انجام داده یا نظارت کرده است را به درستی ارزیابی نکند، در حالیکه آن عضو هنگام شکل‌گیری قضاوت به عنوان بخشی از قرارداد خدمات اعتباردهی، به آن اتکا خواهد کرد.
- ♦ **خطر مشارکت مدیریت** - خطر اینکه یک عضو تیم حسابرسی نقش مدیریت صاحبکار خدمات اعتباردهی را به عهده بگیرد، یا مسئولیت‌های مدیریت صاحبکار خدمات اعتباردهی را انجام دهد.
- ♦ **خطر حمایت (یا مخالفت)** - خطر اینکه یک عضو تیم حسابرسی، منافع یا موقعیت صاحبکار خدمات اعتباردهی را ترویج دهد تا جایی که استقلال وی به خطر بیفتد.

علاوه بر رفتار حرفه ای AICPA، استانداردهای زیر در مورد مراحل پذیرش و ادامه کار با صاحبکار اعمال می‌شود:

- ♦ بخش ۱۰ کنترل کیفیت (QC)، سیستم کنترل کیفیت موسسه که مربوط به حسابرسی است
- ♦ بخش ۲۰۰ AU-C، اهداف کلی حسابرس مستقل و انجام حسابرسی طبق استانداردهای حسابرسی
- ♦ بخش ۲۱۰ AU-C، قرارداد (شرایط کار) حسابرسی
- ♦ بخش ۲۲۰ AU-C، کنترل کیفیت کار انجام شده طبق استانداردهای پذیرفته شده عمومی حسابرسی.<sup>۱</sup>

موضوعات بحث شده در این بخش از رهنمود عملی به بخش‌های زیر تقسیم می‌شوند:

- ♦ بخش ۲: مجموعه مهارت‌ها و صلاحیت‌های حسابرس
- ♦ بخش ۳: مجموعه مهارت‌های مدیریت و صلاحیت‌ها
- ♦ بخش ۴: صلاحیت اخلاقی مدیریت و استراتژی کلی کسب و کار
- ♦ بخش ۵: فرآیندها، کنترل‌ها، از جمله فناوری اطلاعات

هر بخش با خلاصه‌ای از استانداردهای حرفه ای قابل اجرا آغاز می‌شود، سپس برخی از چالش‌های منحصر به فرد کار حسابرسی در اکوسیستم دارایی دیجیتال مشخص می‌شود و با توصیه‌های عملی که ممکن است حسابرسان برای رفع این چالش‌ها و الزامات اعمال کنند، پایان می‌یابد.

## ۲- مجموعه مهارت‌ها و صلاحیت‌های حسابرس

### استانداردهای حرفه ای مرتبط

بخش ۱۰ QC و بخش ۲۲۰ AU-C<sup>۲</sup> هر کدام شامل الزامات مربوط به ارزشیابی موسسه از صلاحیت پرسنل خود برای انجام کار حسابرسی قبل از پذیرش و ادامه کار با صاحبکار و یا حسابرسی ویژه است.

<sup>۱</sup> تمام بخشهای QC و AU-C های فوق را می‌توان در استاندارد حرفه ای AICPA و استانداردهای حسابرسی ایران یافت .

<sup>۲</sup> بندهای ۳۵ الی ۴۰ استاندارد کنترل کیفیت ۱ و ۱۴ الی ۱۸ استاندارد حسابرسی ۲۲۰ ایران.

ارزیابی یک موسسه به طور کلی شامل صلاحیت، توانایی‌ها، منابع و در دسترس بودن تیم حسابرسی است. در این زمینه، تیم حسابرسی شامل شریک حسابرسی، پرسنل موسسه که برای کار حسابرسی اختصاص یافته‌اند (از جمله کارشناسان درون سازمانی) و کارشناسان برون سازمانی در صورت نیاز، می‌باشند.

آیین رفتار حرفه ای AICPA مفهوم اصطلاح صلاحیت را توضیح داده است، بیان داشته:

۰۳- صلاحیت از ترکیب آموزش و تجربه بدست می‌آید، این کار با تسلط بر دانش مشترک مورد نیاز برای تعیین به عنوان حسابدار رسمی آغاز می‌شود. حفظ صلاحیت نیازمند تعهد به یادگیری و پیشرفت حرفه-ای است که باید در طول زندگی حرفه ای یک عضو ادامه یابد. در تمام کارهای حسابرسی و در تمام مسئولیت‌ها، هر یک از اعضا باید متعهد شوند که به درجه‌ای از صلاحیت دست یابند که اطمینان حاصل شود کیفیت خدمات این عضو سطح بالایی از حرفه‌ای‌گری مورد نیاز این اصول را برآورده می‌کند. این مسئولیت فردی یک عضو است.

۰۴- صلاحیت، نشان دهنده دستیابی و حفظ سطحی از شناخت و دانش است که یک عضو را قادر می‌سازد با سهولت و فراست، خدمات ارائه دهد. این موضوع همچنین محدودیت‌های مربوط به توانایی‌های یک عضو را با تاکید بر لزوم مشاوره یا ارجاع کار در مواقعی که کارحسابرسی حرفه‌ای از صلاحیت شخصی یک عضو یا موسسه حسابرسی فراتر است را نیز تعیین می‌کند. هر یک از اعضا، مسئول ارزیابی صلاحیت خود در باره اینکه آیا تحصیلات، تجربه و قضاوت آنها برای مسئولیت پذیری کافی و مناسب است، می‌باشند.

بخش ET ۰,۳۰۰,۰۶۰، "مراقبت حرفه ای"

هدف از ارزیابی موسسه فراهم کردن اطمینان معقول در مورد این موضوع است که تنها کارهای حسابرسی و روابط صاحبکارانی پذیرفته شود که برای آنها، انجام حسابرسی طبق استانداردهای بین المللی و الزامات قانونی و نظارتی قابل اجرا است تا بتوان گزارش حسابرسی که متناسب با شرایط است، صادر نمود.

در نظر گرفتن اینکه آیا موسسه صلاحیت، توانایی و منابع لازم برای انجام کار حسابرسی جدید برای صاحبکار جدید یا صاحبکار موجود را دارد، شامل بررسی الزامات ویژه کار حسابرسی و مشخصات شریک و کارکنان موجود در تمام سطوح مربوط است، از جمله اینکه آیا:

- ♦ پرسنل موسسه دارای دانش مربوط به صنایع یا موضوعات مربوط یا توانایی دستیابی اثر بخش به دانش لازم هستند.
- ♦ پرسنل موسسه تجربه الزامات قانونی یا گزارشگری مربوط یا توانایی دستیابی اثر بخش به صلاحیت-های لازم را دارند.
- ♦ این موسسه پرسنل کافی با صلاحیت‌ها و توانایی‌های لازم را دارد.
- ♦ در صورت نیاز، کارشناسان ذیصلاح در دسترس هستند.
- ♦ افرادی که معیارها و شرایط لازم را برای انجام بررسی کنترل کیفیت کار حسابرسی دارند، در صورت لزوم در دسترس هستند، و
- ♦ موسسه می تواند در مهلت گزارشگری، کار حسابرسی خود را تکمیل کند.

ارزیابی این موارد قبل از پذیرش یک کار حسابرسی یا ادامه کار، به منظور کاهش ریسک پذیرش کار حسابرسی زمانی که موسسه قادر به انجام اثر بخش آن کار نیست، انجام می‌شود. اگر یک موسسه در زمان پذیرش صاحبکار شناخت کافی از صنعت و محیط نداشته باشد و نتواند نیاز به منابع یا آموزش اضافی را مشخص و برطرف کند، انجام کار حسابرسی اثر بخش یا مطابق با استانداردهای حرفه‌ای قابل اجرا، برای آن موسسه دشوار خواهد بود و ممکن است امکانپذیر نباشد.

توانایی حسابرس برای به دست آوردن شناخت کامل از صاحبکار و محیط آن (بخش ۳ و ۴)، از جمله سیستم کنترل داخلی آن (بخش ۵)، برای ارزیابی موثر ریسک و برخورد حسابرسی مهم است. به عنوان مثال، ممکن است یک موسسه تجربه عمیقی در صنعت خدمات مالی داشته باشد و ممکن است با یک صاحبکار در آن صنعت مواجه شود که دارای دارایی‌های دیجیتال نیز باشد. ملاحظات در ارزیابی پذیرش صاحبکار و تعیین ادامه کار، شامل (۱) تخصص صنعت فعلی، (۲) شناخت دارایی‌های دیجیتال؛ و (۳) شناخت چگونگی استفاده از دارایی‌های دیجیتال در

<sup>۳</sup> -مشابه با بند ۳۰ استاندارد کنترل کیفیت ۱ ایران

شرایط صاحبکار ویژه که در حال ارزیابی شدن است، می‌باشد. دانش هر سه مولفه برای یک حسابرس برای عملکرد اثر بخش یک کار حسابرسی لازم است، و ارزیابی توانایی انجام هر یک برای تصمیم‌گیری آگاهانه پذیرش یا ادامه کار صاحبکار، مهم است.

انجام حسابرسی در اکوسیستم‌های دیجیتالی ممکن است ایجاب کند که یک موسسه سیستم کنترل کیفیت موجود خود را به روز کند یا نظارت بیشتری بر آن داشته باشد. به عنوان مثال، اگر موسسه قصد دارد کار حسابرسی را برای موسساتی که مشارکت در اکوسیستم دارند، دنبال کند و برنامه‌های استخدای و آموزشی آن در حال حاضر، موارد منحصر به آن اکوسیستم را در نظر نگیرند، ممکن است ارزیابی اینکه آیا موسسه پرسنل کافی با شایستگی و توانایی لازم در پذیرش صاحبکار یا ادامه آن و سایر فرایندهای کنترل کیفیت یا نیاز به مشارکت کارشناسان برون سازمانی دارد، لازم باشد.

بند A11 بخش ۱۰ QC تایید می‌کند که پرسنل موسسه ممکن است "دانش مربوط به صنایع یا موضوع مربوط یا توانایی کسب اثربخش دانش لازم را نداشته باشند." بنابراین پذیرش صاحبکار و تعیین ادامه کار، مستلزم ارزیابی هر دو خلا در مجموعه مهارت‌های پرسنل موسسه است و اینکه آیا موسسه در صورت انتخاب پذیرش یا ادامه کار با صاحبکار، می‌تواند به طور رضایت بخشی این خلاها را برطرف کند.

علیرغم اینکه استاندارد، امکان دستیابی به دانش لازم برای مسائل و صنایع در حال ظهور مانند دارایی‌های دیجیتالی را فراهم می‌کند، که بنگاه اقتصادی برای آنها تخصص قبلی ندارد، شناخت ریسک اعتماد بیش از حد در تصمیم‌گیری نسبت به پذیرش صاحبکار و ادامه کار، مهم است. بنابراین کنترل‌ها یا نظارت‌های کیفی مناسب موسسه باید برای به چالش کشیدن این تصمیمات انجام شود. اکوسیستم‌های دیجیتالی به سرعت در حال تکامل است. برای موسسه مهم است که سطح تلاش لازم برای کسب دانش در مورد اکوسیستم (یا قسمت‌های مرتبط با آن) را برای تعیین پذیرش و ادامه کار با صاحبکار و انجام صحیح کار حسابرسی انجام دهد.

## چالش‌های خاص دارایی‌های دیجیتالی

رویه‌های پذیرش و ادامه کار با صاحبکار به عنوان ابزاری برای مدیریت و کاهش ریسک‌های شرکای موسسه (شامل تعهدات حرفه‌ای و یا مقررات حسابرسی مستقل) و اطلاع از استراتژی کنترل کیفیت آن برای کار حسابرسی عمل می‌کنند. اگر چه همه صنایع با تغییر روبرو هستند، اکوسیستم‌های دیجیتالی به سرعت در حال پیشرفت است، مجموعه مهارت‌ها و صلاحیت‌های حسابرسان در این محیط ممکن است متشنج شوند. در طراحی روشها برای



مطابقت با الزامات GAAS و بخش ۱۰ QC، موسسات ممکن است در بروزآوری و حفظ مجموعه مهارت‌ها و صلاحیت‌های حساب‌رسان در رابطه با اکوسیستم‌های دارایی‌های دیجیتال با چالش‌هایی به شرح زیر روبرو شوند:

- ♦ مطلع بودن از تحولات نظارتی، صنعتی، فناوری یا گزارشگری مالی که بر صاحبکاران فعلی یا بالقوه تأثیر می‌گذارد و ممکن است ارزیابی ریسک یا سایر جنبه‌های حسابرسی را تحت تأثیر قرار دهد.
- ♦ استخدام، توسعه و حفظ استعدادها در یک بازار کاملاً رقابتی، به ویژه افراد واجد شرایط در فناوری اطلاعات و جنبه‌های امنیت سایبری کار حسابرسی.
- ♦ هدایت، نظارت و بازبینی مناسب تیم کاری حسابرسی، شامل کارکنان، کارشناسان درون سازمانی و ترکیبی از کارشناسان برون سازمانی که مجموعه مهارت‌های آنها ممکن است برای تیم حسابرسی ناآشنا باشد.
- ♦ سازگاری با ریسک‌های جدید یا متفاوت در نتیجه تکامل اکوسیستم یا شناخت مسائل جدید
- ♦ بروزرسانی برنامه‌های آموزشی برای حساب‌رسان فعلی و آتی جهت انطباق با عناصر به سرعت در حال رشد اکوسیستم‌های دارایی‌های دیجیتال، دارایی‌های دیجیتال جدید و محیط تجاری و نظارتی اطراف آن.

هنگام در نظر گرفتن پذیرش یا ادامه کار حسابرسی مطابق با بند ۲۷ بخش ۱۰ QC موسسه چالش‌های داشتن صلاحیت مناسب که قبلاً ذکر شده است را در نظر می‌گیرد.

### ملاحظات خاص روش‌های حسابرسی دارایی‌های دیجیتال

روش‌های خاص برای اکوسیستم‌های دارایی‌های دیجیتال که یک حساب‌رسان ممکن است به عنوان بخشی از فرایند پذیرش کار و ادامه کار حسابرسی انجام دهد، شامل موارد زیر است:

- ♦ تشخیص سیاست یا موضوعات کنترل کیفیت موسسه، انواع صاحبکاران یا کارهای حسابرسی که موسسه قادر به پذیرش آنها است.
- ♦ گستره نواحی تمرکز و یا معیارهای موسسه را برای پذیرش صاحبکارانی که دارای دارایی‌های دیجیتال هستند، مشخص کنید. مثلاً به شرط تحقق معیارهای پذیرش صاحبکار، برخی موسسات ممکن است با توجه به سطح تجربه آنها در حسابرسی تصمیم بگیرند فقط بر واحدهای تجاری اعتبارسنجی تمرکز کنند،

چنین واحد‌هایی، و سایر واحدها، ممکن است در ارائه خدمات به واحدهای تجاری اعتبار سنجی اطمینان داشته باشند. اگر حسابرسان به طور کلی از انواع صاحبکارانی که موسسه می‌پذیرد یا نمی‌پذیرند آگاهی داشته باشند، ریسک کمی وجود خواهد داشت که موسسه قراردادی را که صلاحیت انجام آن را ندارد، قبول کند.

♦ ایجاد دانش عمومی در بین کارکنان موسسه درباره مخاطرات ذاتی اکوسیستم‌های دیجیتال، به گونه‌ای که حسابرسان فعلی این ریسک‌ها و منابع قابل دسترس کار حسابرسی صاحبکاران موجود را درک کنند. به عنوان مثال یک صاحبکار فعلی، ممکن است به روش‌های مختلف، چه از طریق فروشندگان، مشتریان و یا انتخاب‌های استراتژیک شخصی خودش، با اکوسیستم‌های دیجیتال مواجه شود. برای ایجاد چنین دانشی، موسسه می‌تواند یک برنامه آموزشی که در مورد ریسک‌های بیان شده در این رهنمود عملی همراه با روش‌هایی که موسسه در سیستم کنترل کیفیت داخلی خود برای مقابله با این ریسک‌ها، مطرح می‌کند را در نظر بگیرد.

♦ اطلاع‌رسانی منابع مشاوره، آموزش یا راهنمایی را برای کارکنان مرتبط موسسه انجام دهید و در صورت لزوم، تصمیمات ادامه‌کار و پذیرش صاحبکار را براساس واقعیت‌ها و شرایط در حال تغییر، مجدد ارزیابی کنید.

♦ فرد یا افرادی را در داخل یا بیرون از موسسه، با صلاحیت‌های شناخته شده و ثابت شده در موسسات حسابرسی در زمینه اکوسیستم‌های دیجیتال برای ارائه خدمات به عنوان کارشناس (کارشناسان) ذیصلاح (SME)<sup>۴</sup> شناسایی کنید. توجه: ناتوانی در تشخیص چنین فردی ممکن است توانایی موسسه در به دست آوردن صلاحیت لازم برای انجام کار در این محیط را زیر سوال ببرد.

♦ برای ایجاد آگاهی، نام کارشناسان ذیصلاح (SME) را اطلاع‌رسانی کنید.

♦ برای اطمینان از اینکه ملاحظاتی که قبلاً ذکر شده اند به صورت مناسب تنظیم و مستند شده باشند، به مشارکت کارشناسان ذیصلاح (SME) در تصمیم‌گیری در مورد ادامه کار و پذیرش صاحبکار نیاز دارید.

♦ برنامه‌های آموزشی جهت تطبیق کارکنان مرتبط با مسائل و ریسک‌های منحصر به فرد بحث شده در بخش‌های دیگر این رهنمود، متناسب با نیازهای مشخص شده در فرآیند پذیرش صاحبکار را در نظر

<sup>۴</sup> - subject matter expert(s)

بگیرید، منابع AICPA<sup>۵</sup> یا سایر منابع را جهت آموزش متناسب برای کارکنان حسابرسی و کارشناسان درون سازمانی در نظر بگیرید. ( برای مثال، فناوری اطلاعات، ارزیابی و یا امنیت سایبری)

♦ جهت تعیین چارچوب دسترسی کارشناسان برون سازمانی که انتخاب خواهند شد، دستورالعمل‌هایی را برای ارزیابی کارشناسان ایجاد کنید که شاید در گذشته لازم نبوده است. (بند ۹ از بخش ۶۲۰ AU-C، استفاده از نتایج کار کارشناس حسابرسی)<sup>۶</sup>

در صورتیکه یک یا چند کار حسابرسی در رابطه با دارایی‌های دیجیتال پذیرفته شود، ممکن است موسسه نیاز به در نظر گرفتن سایر بروزرسانی‌های احتمالی برای کنترل کیفیت داشته باشد، از جمله انواع تغییرات زیر:

- ♦ اسامی مدیرمسئول کارحسابرسی و سایر افراد تأیید شده را جهت انتصاب برای نقش‌های مختلف در رابطه با حسابرسی اکوسیستم دارایی‌های دیجیتال مشخص کنید. (بخش‌های ۳۳ و ۳۴ از بخش ۱۰ QC)
- ♦ طراحی، پیاده سازی و تعهد به حفظ راهنما، رهنمودهای عملی، ابزارها، آموزش‌ها و برنامه‌های کاری، برای ارتقاء، ثبات و کیفیت در عملکرد کارحسابرسی، نظارت و بازبینی، به ویژه در مرحله ارزیابی ریسک و اجرای طرح کلی حسابرسی در حسابرسی اکوسیستم دارایی‌های دیجیتال (بندهای ۳۵ و ۳۶ از بخش ۱۰ QC)
- ♦ الزامات مشاوره‌ای را برای موارد حسابرسی یا گزارشگری مالی منحصر به فرد که ممکن است به اکوسیستم دارایی‌های دیجیتال مرتبط باشد، ایجاد کنید. (بند ۳۷ از بخش ۱۰ QC)
- ♦ معیارهایی را برای تعیین اینکه کدام یک از کارهای حسابرسی نیازمند بررسی کنترل کیفیت کار حسابرسی، الزامات بررسی متناسب با ریسک‌های جدید یا متفاوت است را بروز رسانی کنید، و صلاحیت فنی و صلاحیت بازرسان تأیید شده را ارزیابی کنید. (بندهای ۴۵ - ۳۸ از بخش ۱۰ QC)
- ♦ برای ارزیابی کیفیت کار حسابرسی و اثربخشی اقدامات کنترل کیفیت شرح داده شده در این رهنمود عملی، کارهای حسابرسی جدید یا پرریسک را در حیطه نظارتی روش‌های کنترل کیفیت قبل یا بعد از صدور گزارش قرار دهید. ( بند ۵۲ از بخش ۱۰ QC)

<sup>۵</sup> - AICPA دوره‌ای با عنوان مبانی ( اصول اساسی) بلاکچین برای گواهینامه حرفه‌ای حسابداری و امور مالی و همچنین یک گزارش هیات دولت با عنوان فناوری بلاکچین و تأثیر بالقوه آن در حرفه حسابرسی و اطمینان بخشی تدوین کرده است.

<sup>۶</sup> مشابه با بند ۸ استاندارد حسابرسی ۶۲۰ ایران استفاده از نتایج کار کارشناس.

علاوه بر رویه‌هایی که قبلاً ذکر شد، موارد زیر برخی از سوالاتی است که یک موسسه ممکن است در فرآیند پذیرش صاحبکار و ادامه کار برای ارزیابی مجموعه مهارت‌ها و صلاحیت‌های خود در نظر بگیرد. برای هرگونه پاسخ منفی یا ناشناخته، حسابرس ممکن است نیاز به انجام مراحل اضافی قبل از قبول یا موافقت با انجام کارحسابرسی داشته باشد، یا نهایتاً صاحبکار یا کارحسابرسی را قبول نکند. این نمونه‌ها نه جامع و نه همیشه قابل اجرا هستند، زیرا واقعیت‌ها و شرایط ممکن است از یک کارحسابرسی به کار دیگر متفاوت باشد.

- ♦ آیا این شرکت مشتریان مشابه دیگری در اکوسیستم دارایی‌های دیجیتال دارد؟
  - ♦ آیا حسابرس از فضای نظارتی قابل اجرا آگاهی دارد و اینکه آیا ریسکی مبنی بر اینکه یک واحد تجاری از قوانین و مقررات پیروی نکند وجود دارد؟
  - ♦ آیا حسابرس درک می‌کند که چارچوب گزارشگری مالی قابل اجرا برای صاحبکار یا عملیات آن چگونه اعمال می‌شود؟
  - ♦ آیا حسابرس برای شناسایی پرسنل مناسب جهت تعیین کردن کارحسابرسی (از جمله شریک، کارکنان و کارشناسان درون سازمانی) و انجام ارزیابی ریسک اثر بخش، عملکرد صاحبکار را به اندازه کافی درک کرده است؟
  - ♦ آیا پرسنل از دانش کافی برخوردارند؟ در غیر این صورت، آیا می‌توان با آموزش‌های بیشتر یا کمک از کارشناسان برون سازمانی این خلاها را برطرف کرد؟
- توجه داشته باشید که این سوالات به توانایی تیم حسابرسی پیشنهادی برای شناخت و تعامل با مدیریت و کارشناسان آن در زمینه‌های دیگر، از جمله دانش کافی برای به چالش کشیدن مواضع مدیریت، اشاره دارد. همانطور که در بخش‌های ۳ تا ۵ اشاره شد، یک موسسه ممکن است نیاز به گفتگوی بیشتر با مدیریت را قبل از پذیرش و ادامه کار صاحبکار لازم بداند، به طور بالقوه سوالاتی در مورد میزان دارایی‌های دیجیتال در عملیات واحد تجاری، سیستم کنترل داخلی واحد تجاری در ارتباط با دارایی‌های دیجیتال، واحد تجاری از چه ابزاری استفاده می‌کند، معاملات را چگونه ارزیابی و ثبت می‌کند یا از چه راهکارهایی برای محافظت و نگهداری استفاده می‌کند. بعلاوه، این سوالات ممکن است حسابرس را در ارزیابی پرسنل حسابرسی و مجموعه مهارت‌های مناسب یاری دهد.

- ♦ آیا پرسنل وقت و منابع لازم برای انجام اثر بخش کار حسابرسی را دارند؟  
توجه داشته باشید که حتی در صورت استفاده از کارشناسان برون سازمانی، الزامات اخلاقی مربوط به مراقبت‌های تخصصی و حرفه ای (بخش ۰,۳۰۰,۰۶۰ ET) و GAAS مستلزم این است که موسسه رویه‌هایی را برای نظارت و پذیرش مسئولیت برای کفایت کار حسابرسی در اختیار داشته باشد. علاوه بر این، در این زمینه، "منابع" ممکن است شامل سرمایه گذاری در فناوری یا ابزارهای مورد نیاز برای جمع آوری شواهد حسابرسی کافی و مناسب از دارایی‌ها و معاملات دیجیتال باشد. معمولا، ممکن است شامل منابع ارزیابی و اعتبارسنجی مبادلات باشد.
- ♦ آیا موسسه فرایندها و منابع مناسبی برای پشتیبانی تیم حسابرسی پیشنهادی با توجه به سوالات، مشاوره یا بازبینی پیش از صدور گزارش در اختیار دارد؟  
همانطور که قبلاً توضیح داده شد، ممکن است موسسات برای ارائه راهنمایی یا منابع بیشتر برای مشاوره یا رویه‌های بازبینی پیش از صدور گزارش، از جمله بررسی کنترل کیفیت کار حسابرسی، نیاز به تغییر شیوه‌های کنترل کیفیت موجود داشته باشند. علاوه بر ارائه آموزش و منابع به تیم حسابرسی، ممکن است موسسات برای پرسنلی که عملیات بازبینی و مشاوره را انجام می دهند نیز لازم باشد این کار را انجام دهند.

### ۳- مجموعه مهارت‌های مدیریت و صلاحیت‌ها

#### استانداردهای حرفه ای مرتبط

بخش ۷، AU-C۲۱۰، حسابرس را در به بدست آوردن توافقی با مدیریت که مسئولیت خود را بپذیرد ملزم می‌کند.

- الف - تهیه و ارائه منصفانه صورتهای مالی مطابق با چارچوب گزارشگری مالی پذیرفته شده
- ب - طراحی، اجرا و نگهداری کنترل داخلی مربوط به تهیه و ارائه منصفانه صورتهای مالی که عاری از تحریف با اهمیت باشد، چه به دلیل تقلب یا اشتباه و
- ج - دسترسی حسابرس به کلیه اطلاعات و افراد مرتبط لازم برای بدست آوردن شواهد حسابرسی

<sup>۷</sup> مشابه استاندارد حسابرسی ۲۱۰ ایران قرارداد حسابرسی.

به علاوه، همانطور که در بخش ۴ توضیح داده شده است، در نظر گرفتن برخی از الزامات بخش ۳۱۵ AU-C، شناخت واحد تجاری و محیط آن و ارزیابی تحریف‌های با اهمیت، و بخش ۲۵۰ AU-C، در نظر گرفتن قوانین و مقررات در حسابرسی صورت‌های مالی، در فرآیند پذیرش و ادامه کار با صاحبکار مفید است. به همین ترتیب، حسابرسان ممکن است رویه‌هایی را برای شناخت تعهد و صلاحیت مدیریت در مورد برخی مشاغل خاص و چگونگی دستیابی به سطوح مهارت‌ها و دانش لازم، اعمال کنند. حسابرس همچنین باید ویژگی‌های ارکان راهبری، مانند سمت و تجربه آنها و اینکه آیا آنها مهارت و دانش کافی برای انجام مسئولیت‌های خود را دارند، در نظر بگیرد.

### چالش‌های خاص دارایی‌های دیجیتال

با توجه به پیچیدگی مرتبط با فناوری بلاکچین و دارایی‌های دیجیتال، مدیریت ممکن است فاقد مجموعه مهارت‌ها یا صلاحیت‌های لازم برای ثبت و نگهداری اسناد و مدارک واحد تجاری و محافظت از دارایی‌های باشد. بنابراین، ارزیابی اینکه آیا پرسنل واحد تجاری از صلاحیت‌ها و توانایی‌های لازم برخوردار هستند، احتمالاً یک فاکتور مهم مرتبط با تصمیم حسابرس برای پذیرش یا ادامه یک کار حسابرسی می‌باشد. حتی اگر مدیریت از صلاحیت اخلاقی و استراتژی مناسب کسب و کار برخوردار باشد، اما از مجموعه مهارت‌ها و صلاحیت‌های فنی مناسب برخوردار نباشد، ممکن است، کار حسابرسی بدون توجه به این کمبودها امکان پذیر نباشد. دلیل این امر ممکن است این باشد که دفاتر و اسناد و مدارک به طور مناسب نگهداری نمی‌شوند، فرایندها و کنترل‌ها اجرا نشده اند، یا مدیریت بیش از حد به حسابرس اعتماد می‌کند، در نتیجه این ریسک را ایجاد می‌کند که حسابرس قادر به انجام مسئولیت خود در زمینه ارائه نظر مستقل در مورد صورت‌های مالی واحد تجاری نباشد.

همچنین، هنگام ارزیابی ریسک‌های مربوط به دوره مورد پذیرش یا ادامه کار، شناخت اینکه چه زمان مدیریت مجموعه مهارت‌ها و شایستگی‌های لازم را کسب کرده بسیار مهم است. به عنوان مثال، اگر یک واحد تجاری اخیراً دارایی‌های دیجیتال را در عملیات خود گنجانده است، ممکن است برای حسابرس مهم باشد که توانایی مدیریت در پیاده‌سازی سیستم‌ها، فرآیندها و کنترل دارایی‌های دیجیتال را برای ارائه صورت‌های مالی عاری از تحریف با اهمیت، لحاظ نماید. به طور مشابه، اگر در هنگام وقوع یک معامله یا فعالیت کنترلی اقدامات خاصی انجام نشود، به دست آوردن انواع خاصی از شواهد حسابرسی ممکن است دشوار باشد (به عنوان مثال شواهدی مبنی بر اینکه کنترل‌های مدیریت مربوط به کلید خصوصی به طور اثربخش کار می‌کند یا خیر) همچنین، توانایی‌های فنی واحد تجاری در توسعه فناوری‌های دارایی‌های دیجیتال، نیز مهم است.

مجموعه مهارت‌های لازم و صلاحیت‌های مدیریت شامل درک عمومی مدیریت از مجموعه مهارت‌های فنی مربوط به فناوری بلاکچین و دارایی‌های دیجیتال است، برای مدیریت کافی است که موارد زیر را انجام دهد:

- ♦ ریسک‌های منحصر به فرد موجود در محیط را شناسایی کرده و کنترل‌های داخلی را برای برخورد با چنین ریسک‌هایی طراحی و پیاده سازی کنید. به عنوان مثال، با توجه به ناشناس بودن هویت<sup>۸</sup> در ارتباط با دارایی‌های دیجیتال، مدیریت ممکن است کنترل‌های داخلی را برای شناسایی اشخاص وابسته و روابط و معاملات با اشخاص وابسته پیاده سازی کند. به عنوان مثال، شناخت صاحبکار، یکی از رویه‌های کنترلی مهم است.
- ♦ سرعت پیشرفت فناوری و نیاز به کنترل‌های بیشتر یا نیاز به تعداد کارکنان بیشتر را بشناسید.
- ♦ برای نگهداری دفاتر و اسناد و مدارک مناسب، از جمله حفاظت و پشتیبانی مناسب از معاملات و استفاده از چارچوب گزارشگری مالی مناسب، فرایندها و کنترل‌هایی داشته باشید. به عنوان مثال، یک واحد تجاری ممکن است سابقه مستقلى در مورد معاملات دارایی دیجیتال داشته باشد و آن را با خلاصه معاملات ارائه شده توسط متصدی نگهداری، مغایرت‌گیری نماید.
- ♦ پرسنل واجد شرایطی داشته باشید که توانایی استفاده مناسب از چارچوب گزارشگری مالی را داشته باشند.
- ♦ قوانین و مقررات قابل اجرا یا حوزه‌های قوانین و مقررات در حال تکمیل را شناسایی کنید.
- ♦ دسترسی یا توانایی شناسایی نیاز به کارشناسان را داشته باشید. به عنوان مثال، مشاور حقوقی ذیصلاح، کارشناس فناوری اطلاعات یا کارشناس امنیت سایبری.

## ملاحظات خاص روش‌های حسابرسی دارایی‌های دیجیتال

با توجه به چالش‌هایی که قبلاً شرح داده شد، ارزیابی مجموعه مهارت‌ها و شایستگی‌های مدیریت در فرآیند پذیرش یا ادامه کار با صاحبکار می‌تواند بیشتر از آنچه معمولاً برای سایر صاحبکاران جدید یا ادامه کار انجام می‌شود،

<sup>۸</sup> در محیط‌های بلاکچین، دارایی‌های دیجیتال بین آدرس‌های بلاکچین مبادله می‌شوند و از کلیدهای خصوصی برای اعطای مجوز استفاده می‌شود. با این حال، نام و هویت مشخص طرفین معامله صریحاً با آن آدرس‌ها و کلیدها مشخص نیست. اگرچه تعیین هویت از طریق روش‌های مختلف بازشناسی شخصی امکان پذیر است، اما با معامله و بدون ارائه اطلاعات قابل شناسایی شخصی، هویت اشخاص پنهان می‌ماند.

چالش برانگیز باشد. رویه‌های پذیرش و ادامه کار با صاحبکار ممکن است شامل ارزیابی این موضوع باشد که آیا مدیریت شناخت لازم از ریسک‌ها، کنترل‌های لازم و چارچوب گزارشگری مالی قابل اجرا دارد یا خیر. این موضوع شامل ارزیابی توانایی واحد تجاری در شناسایی و رسیدگی به ریسک‌های موجود در فناوری زیربنایی است که ممکن است ریسک تحریف با اهمیت را به دلیل اشتباهات یا تقلب ایجاد کند.

موارد زیر برخی از سوالات یک حسابرس است که ممکن است در ارزیابی فرآیند پذیرش و ادامه کار برای ارزیابی مجموعه مهارت‌ها و توانایی‌های مدیریت در نظر گرفته بگیرد.

♦ آیا مدیریت در اکوسیستم دارایی‌های دیجیتالی تجربه‌ای دارد که بتواند ریسک‌های منحصر به فرد موجود در این محیط را شناسایی کرده و کنترل‌های داخلی را برای پاسخگویی به چنین ریسک‌هایی طراحی و اجرا کند (به عنوان مثال، ریسک‌های مربوط به مدیریت کلید خصوصی، معاملات و افشای اشخاص وابسته یا سایر ریسک‌های تقلب)؟

♦ آیا مدیریت محیط نظارتی قابل اجرا و حوزه‌های قوانین و مقررات در حال تکامل را درک می‌کند؟

♦ آیا مدیریت (۱) دفاتر و اسناد و مدارکی را به صورت مستقل از بلاکچین یا شخص ثالث نگهداری می‌کند یا (۲) سوابق واحد تجاری را فقط از بلاکچین یا اظهارات ارائه شده توسط شخص ثالث بدست می‌آورد؟ اگر مورد دوم باشد، ممکن است حسابرس بخواهد به عنوان بخشی از فرآیند پذیرش و ادامه کار، فرایندهای مدیریت و کنترل کیفیت اضافی مربوط به این اطلاعات را بیشتر بشناسد.

♦ آیا مدیریت، کارشناسان ذیصلاح یا مشاوران حسابداری مناسب و واجد شرایط را در صورت لزوم، زمانی که مدیریت، دانش یا تخصص کافی ندارد به کار می‌گیرد، (به عنوان مثال، مشاور حقوقی درون سازمانی یا کارشناسان فناوری اطلاعات، از جمله کارشناسان رمزنگاری و امنیت سایبری) و ارزیابی‌های اثربخش از کار انجام شده توسط چنین کارشناسانی را انجام می‌دهد؟

♦ آیا مدیریت چگونگی اعمال چارچوب گزارشگری مالی قابل اجرا بر عملکردهایش را درک می‌کند؟ (به بخش "زیر گروه حسابداری" این رهنمود عملی مراجعه کنید.)

علاوه بر سوالات قبلی، مطالعه دستورالعمل رویه‌های حسابداری تهیه شده توسط واحد تجاری (یا انجام سوال‌های دقیق از مدیریت) به حسابرس برای تعیین اینکه آیا واحد تجاری علاوه بر اینکه از استانداردهای حسابداری به درستی استفاده کرده است، دانش کافی برای ارزیابی کاربرد استانداردهای حسابداری را دارد یا خیر، کمک می‌کند. واحد تجاری باید اعضاء دارای صلاحیت در گروه‌های مالی و حسابداری، برای تعیین برخورد حسابداری مناسب با



دارایی‌های دیجیتال را داشته باشد. دارایی‌های دیجیتال ممکن است ویژگی‌های مختلفی داشته باشند که طبقه بندی‌های مختلف در صورت‌های مالی را ایجاب می‌کنند. برای ارزیابی شناسایی، عدم شناسایی، اندازه گیری، طبقه بندی و ردیابی به موقع و مناسب دارایی‌های دیجیتال جدید، فرایندهایی باید در نظر گرفته شوند (به بخش "زیر گروه حسابداری" این رهنمود عملی مراجعه کنید).

بسته به نتایج این سوالات و رویه‌ها، حساب‌برسان ممکن است نیاز به سوالات یا جستجوی اطلاعات بیشتر داشته باشند. حساب‌برس علاوه بر ارزیابی مجموعه مهارت‌ها و صلاحیت‌های مدیریت، صلاحیت اخلاقی مدیریت و استراتژی کلی کسب و کار راجع به دارایی‌های دیجیتال را بخشی از فرآیند پذیرش و ادامه کار می‌داند.

#### ۴- صلاحیت اخلاقی مدیریت و استراتژی کلی کسب و کار

##### استانداردهای حرفه‌ای مرتبط

مطابق با بند ۲۷ بخش ۱۰ QC، موسسه باید سیاست‌ها و رویه‌هایی را برای پذیرش و ادامه کار با صاحبکار و قرارداد حسابرسی ایجاد کند، و روش‌هایی برای اینکه موسسه اطمینان معقول حاصل کند که پذیرش یا ادامه روابط و کارهای حسابرسی، فقط در مواردی که موسسه درستکاری صاحبکار را در نظر گرفته باشد و اطلاعاتی نداشته باشد که بتواند به این نتیجه برسد که صاحبکار فاقد درستکاری است، طراحی کند.

مواردی که باید در مورد درستکاری صاحبکار در نظر گرفته شود شامل موارد زیر است:<sup>۹</sup>

<sup>۹</sup> مشابه با بند ۲۸ استاندارد کنترل کیفیت ۱ ایران.

- ♦ هویت و شهرت تجاری مالکان اصلی صاحبکار، هیئت مدیره و مدیران اجرایی.
- ♦ ماهیت عملیات صاحبکار، شامل رویه‌های تجاری آن
- ♦ اطلاعاتی درباره نگرش مالکان اصلی صاحبکار، هیئت مدیره و مدیران اجرایی درباره موضوعاتی مانند کنترل داخلی یا گزارشگری مطابق با استانداردهای حسابداری
- ♦ نشانه‌های محدودیت غیر متعارف در دامنه کاری
- ♦ مواردی که نشان می‌دهد صاحبکار ممکن است در پولشویی یا سایر فعالیت‌های مجرمانه نقش داشته باشد.
- ♦ دلایل پیشنهاد انتخاب موسسه و عدم انتخاب مجدد موسسه قبلی (بند A۱۲ از بخش ۱۰ QC).

همچنین ممکن است برای حسابرس هنگام انجام مراحل پذیرش و ادامه کار، مفید باشد که در سایر بخش‌های AU-C در مورد فعالیت‌هایی که ممکن است پس از پذیرش و ادامه کار با صاحبکار اتفاق بیفتد، موارد خاصی را بررسی کند، مانند بخش ۳۱۵ و ۲۵۰ AU-C. به عنوان مثال، بند ۱۲ از بخش ۳۱۵ AU-C،<sup>۱۰</sup> حسابرس را ملزم به شناخت اهداف و راهبردهای واحد تجاری و ریسک‌های مربوط به تجارت و صنعت آن واحد می‌کند که ممکن است منجر به ایجاد تحریف بااهمیت شود. بند ۱۵ از بخش ۳۱۵ AU-C همچنین ایجاب می‌کند که حسابرس باید شناختی از محیط کنترلی داشته باشد، از جمله ارزیابی اینکه آیا: ۱۱

- ♦ مدیران اجرایی، با نظارت ارکان راهبری، فرهنگ درستکاری و رفتار اخلاقی را ترویج و حفظ کرده اند، و
- ♦ نقاط قوت عناصر محیط کنترلی در مجموع، بستر مناسبی برای سایر اجزای کنترل داخلی فراهم می‌کند، و اینکه آیا سایر اجزای کنترل داخلی در اثر نارساییهای محیط کنترلی، آسیب می‌بینند یا خیر.

عناصر محیط کنترلی که ممکن است هنگام بدست آوردن این شناخت مربوط باشند شامل ارتباطات مدیریت و الزام اجرایی درستکاری و ارزشهای اخلاقی و تعهد به صلاحیت و همچنین ویژگیهای ارکان راهبری مانند تجربه و حسن شهرت آنها هستند. ( بند . A۷۹ از بخش ۳۱۵ AU-C)<sup>۱۲</sup>

<sup>۱۰</sup> مشابه بند ۱۱ استاندارد حسابرسی ۳۱۵ تشخیص و ارزیابی خطرهای تحریف بااهمیت از طریق شناخت واحد تجاری و محیط آن.  
<sup>۱۱</sup> مشابه بند ۱۴ استاندارد حسابرسی ۳۱۵ تشخیص و ارزیابی خطرهای تحریف بااهمیت از طریق شناخت واحد تجاری و محیط آن  
<sup>۱۲</sup> مشابه بند ت-۷۷ استاندارد حسابرسی ۳۱۵ تشخیص و ارزیابی خطرهای تحریف بااهمیت از طریق شناخت واحد تجاری و محیط آن.

حسابرسان همچنین ممکن است الزامات بخش ۲۵۰ AU-C را که جنبه‌های محیط قانونی و مقرراتی را برجسته می‌کند، در نظر بگیرند. بند ۱۲۰ بخش ۲۵۰ AU-C<sup>۱۳</sup> مستلزم آن است که حسابرس شناخت کلی از موارد زیر را بدست آورد:

الف- چارچوب قانونی و مقرراتی حاکم بر واحد تجاری و صنعت یا بخشی که واحد تجاری در آن فعالیت می‌کند، و

ب- چگونگی رعایت این قوانین و مقررات توسط واحد تجاری.

### چالش‌های خاص دارایی‌های دیجیتال

اکوسیستم دارایی دیجیتال ملاحظات منحصر به فردی را برای حسابرسان در فرآیند پذیرش و ادامه کار با صاحبکار ارائه می‌دهد، که هم به درستکاری و تعهد مدیریت به انطباق با قوانین و مقررات و هم به اهداف استراتژیک آن مربوط می‌شود. به عنوان مثال، موارد زیر:

- ♦ ناشناس بودن هویت در معاملات دارایی‌های دیجیتال ممکن است فرصتی را برای فعالیت‌های غیرقانونی مانند پولشویی یا سایر فعالیت‌های غیرقانونی فراهم کند. عدم انطباق با رویه‌های شناخت صاحبکار، روش‌های مبارزه با پولشویی و سایر مقررات می‌تواند ریسک تجاری قابل توجهی را به عنوان جریمه و مجازات اعم از کیفری و مدنی برای واحد تجاری ایجاد کند.
- ♦ به دلیل ناشناس بودن هویت شرکت‌کنندگان در معاملات بلاکچین عمومی ممکن است شناسایی معاملات با اشخاص وابسته یا "کاربران بد (هکرها)" که ممکن است قصد غیرقانونی یا کلاهبرداری داشته باشند دشوار باشد. همچنین ممکن است فرصت‌هایی را برای درگیر شدن در طرح‌های کلاهبرداری مانند معاملات دوسویه فراهم کند.
- ♦ سهولت ورود به بازار (یعنی هر شخصی می‌تواند یک دارایی دیجیتال را داد و ستد کند یا ایجاد کند) ممکن است کسانی را که فاقد درستکاری یا فاقد تعهد به صلاحیت هستند را به اکوسیستم دارایی‌های دیجیتال جذب کند.

<sup>۱۳</sup> مشابه بند ۱۲ استاندارد حسابرسی ۲۵۰ ایران / ارزیابی رعایت قوانین و مقررات در حسابرسی صورتهای مالی.

♦ ممکن است مدیریت شناخت کافی از دارایی‌های دیجیتال، فناوری و دستورالعمل‌های اساسی یا محیط نظارتی در حال توسعه برای شناسایی ریسک‌های مربوط به کلاهبرداری یا عدم انطباق با قوانین و مقررات نداشته باشد. بعلاوه، اگرچه ممکن است مدیریت ادعا کند که فعالیت‌های مربوط به دارایی‌های دیجیتال ممکن است برای صورتهای مالی قابل توجه نباشند اما برای حسابرس مهم است که هنگام انجام ارزیابی پذیرش صاحبکار و ادامه کار، عدم انطباق با قوانین و مقررات (به عنوان مثال عدم رعایت الزامات نظارتی مربوط به صدور توکن که ممکن است یک "اوراق بهادار" باشد) را در نظر بگیرد.

### روش‌ها برای توجه خاص به دارایی‌های دیجیتال

هنگام تصمیم‌گیری برای پذیرش و ادامه کار با صاحبکار، برای حسابرسی واحدهای تجاری موجود در اکوسیستم دارایی دیجیتال، حسابرسان احتمالاً دریافت اطلاعات لازم برای شناخت استراتژی تجاری واحد تجاری، عملیات برنامه ریزی شده و نقشی را که واحد تجاری در کل اکوسیستم دارایی‌های دیجیتال ارائه می‌کند یا قصد دارد ارائه کند، مهم می‌دانند.

کسب شناخت از هدف واحد تجاری در مشارکت اولیه آن یا تغییرات قابل توجه در مشارکت آن در دارایی‌های دیجیتال، یک جنبه اساسی در ارزیابی درستکاری مدیریت است. اگر یک کار حسابرسی جدید پذیرفته شود یا یک کار حسابرسی موجود ادامه یابد، چنین شناختی نقطه شروع حیاتی جهت تشخیص و ارزیابی ریسک‌های تحریف بااهمیت مربوط به قسمت‌هایی است که ممکن است بررسی ویژه حسابرسی را نیاز داشته باشد (به عنوان مثال، معاملات با اشخاص وابسته).

علاوه بر این، هر نقشی در اکوسیستم دارایی دیجیتال (به عنوان مثال واحد تجاری که دارایی‌های دیجیتال را نگهداری می‌کنند، متصدیان نگهداری یا شرکت‌های کیف پول‌ها، صرافی‌ها، صندوق‌هایی که در دارایی‌های دیجیتال سرمایه گذاری می‌کنند، فروشندگانی که ارز دیجیتال را قبول می‌کنند و اعتبارسنج‌ها) ممکن است ملاحظات منحصر به فردی را ارائه دهند.

با توجه به چالش‌های توصیف شده، حسابرسان با توجه به پذیرش کار حسابرسی جدید یا ادامه کار حسابرسی موجود برای صاحبکاران در اکوسیستم دارایی دیجیتال، معمولاً افزایش روش‌های معمول خود را در نظر گرفتن برخی یا تمام موارد زیر مناسب می‌دانند. (نمونه‌های ارائه شده جامع و کامل نیستند و ماهیت و میزان این

روشهای نمونه ممکن است بسته به نقش واحد تجاری در اکوسیستم و نوع دارایی‌های دیجیتال در دست واحد تجاری متفاوت باشد).

- ♦ برای شناخت هدف واحد تجاری در رابطه با قرارداد فعلی و آتی، در دارایی‌های دیجیتال، از مدیریت پرس و جو کنید. عمق و گستردگی این پرس و جوها ممکن است بسته به ماهیت و اهمیت مشارکت واحد تجاری در دارایی‌های دیجیتال متفاوت باشد (به عنوان مثال، اینکه مالک، سرمایه گذار، طرف معامله واحد تجاری، مسئول نگهداری دارایی‌های دیجیتال و یا معامله آنها است) به عنوان مثال، اگر واحد تجاری پرداخت در دارایی‌های دیجیتال را بپذیرد اما بلافاصله آن را به دلار آمریکا تبدیل کند، ملاحظات حسابرس درباره هدف واحد تجاری از مشارکت در دارایی‌های دیجیتال ممکن است در مقایسه با صرافی که انواع مختلفی از دارایی‌های دیجیتال را ارائه می دهد، پیچیده تر باشد.
- ♦ برای شناخت محیط کنترلی و فضای اخلاقی در رده بالای سازمان، از جمله فلسفه مدیریت، سبک عملیات و سطح تحمل ریسک، از مدیریت پرس و جو کنید. این پرس و جوها ممکن است به منظور شناخت این که چگونه مشارکت واحد تجاری در دارایی‌های دیجیتال به عنوان بخشی از ارزیابی ریسک مدیریت و میزان ریسکی که آنها مایل به پذیرش در شرایط ریسک پذیری کلی خود هستند، در نظر گرفته شده است.
- ♦ برای شناخت ماهیت دارایی‌های دیجیتال نگهداری شده یا در نظر گرفته شده برای نگهداری و اهمیت این دارایی‌ها برای کسب و کار از مدیریت پرس و جو کنید. پرس و جوها ممکن است به شناخت درستی از نوع دارایی‌های دیجیتال موجود در واحد تجاری و اهمیت این دارایی‌ها بپردازد.
- ♦ برای شناخت سیاست‌ها و روش‌های آنها در مورد کار با مشتریان جدید یا برقراری ارتباط با سایر نقش آفرینان در اکوسیستم دارایی‌های دیجیتال، از مدیریت پرس و جو کنید این پرس و جوها ممکن است شامل روش‌های شناخت صاحبکار، روش‌های پولشویی و سایر اقدامات احتیاطی لازم برای شناخت هویت و درستکاری طرف مقابل باشد. این رویه‌ها همچنین می توانند به شناخت درستی از فرآیند مدیریت برای شناسایی اشخاص و روابط وابسته و معاملات با اشخاص وابسته کمک کنند. پرس و جوها ممکن است فراتر از مدیر اجرایی، مدیر ارشد مالی و مدیر ارشد حسابداری باشد و در صورت لزوم شامل بحث و گفتگو با مدیران ارشد کنترلی، مدیریت ریسک یا دپارتمان حقوقی واحد تجاری یا مدیران ارشد مبارزه با پولشویی باشد.

- ♦ برای شناخت فرآیندها و رویه‌های آنها برای نظارت بر معاملات مربوط به فعالیت غیرقانونی یا مشکوک پس از معارفه و مباشرت با صاحبکاران جدید یا وارد شدن به یک رابطه کسب و کار جدید، از مدیریت پرس و جو کنید. این موضوع می‌تواند شامل پرس و جو برای شناخت اشخاص ثالثی باشد که ممکن است برای تسهیل معاملات دارایی دیجیتال (به عنوان مثال صرافی ارز دیجیتال) از آنها استفاده شود.
- ♦ از مدیریت پرس و جو کنید تا شناخت درستی از چارچوب قانونی و نظارتی قابل اجرا در معاملات دارایی دیجیتال، از جمله مقررات در سایر حوزه‌هایی که واحد تجاری در آن مشغول به کار است، تغییرات در این محیط و فرآیند مدیریت برای حفظ انطباق با الزامات قانونی و نظارتی را کسب کنید.
- ♦ در مورد قوانین بانکی یا قانون پولشویی، گزارش‌های تهیه شده توسط شخص ثالث یا مستندات فرآیند تهیه شده توسط واحد تجاری را از مدیریت پرس و جو کنید. حسابرس می‌تواند پرس و جو کند که آیا موارد شناخته شده عدم مطابقت با این قوانین و مقررات رخ داده است یا اینکه واحد تجاری از نهادهای نظارتی در مورد انطباق یا عدم انطباق واحد تجاری با این نوع قوانین و مقررات گزارشی دریافت کرده است.
- ♦ برای شناخت سیاست‌ها و روش‌ها، از جمله روش‌های کافی، هنگام ارزیابی دارایی‌های بالقوه دیجیتال برای انجام معامله، از مدیریت پرس و جو کنید. عمق و گستردگی این پرس و جوها ممکن است بسته به نقش در اکوسیستم و نوع دارایی دیجیتال متفاوت باشد (به عنوان مثال، یک دارایی دیجیتال معتبر ممکن است در مقایسه با دارایی دیجیتال کمتر شناخته شده یا دارای نقدینگی کمتر، دارای ریسک متفاوتی باشد).
- ♦ برای شناخت سیاست‌ها و رویه‌های واحد تجاری برای شناسایی اشخاص وابسته و معاملات با اشخاص وابسته از مدیریت پرس و جو کنید. با توجه به ناشناس بودن هویت شرکت‌کنندگان در معاملات بلاکچین، خطر سوء استفاده‌های اساسی مرتبط با معاملات و افشای اشخاص وابسته و همچنین ریسک انجام فعالیت‌های متقلبانه (به عنوان مثال، انجام معاملات با اشخاص وابسته برای افزایش درآمد) ممکن است افزایش یابد. دستیابی به شناختی از سیاست‌ها و رویه‌های مدیریت برای شناسایی اشخاص وابسته و معاملات با اشخاص وابسته، ممکن است حسابرس را در ارزیابی تعهد واحد تجاری برای توسعه فرهنگ اخلاقی از طریق اجرای فرایندها و کنترل‌ها یاری کند.
- ♦ برای شناخت ملاحظات مربوط به نگهداری دفاتر، اسناد و مدارک کافی مرتبط با دارایی‌های دیجیتال که واحد تجاری در حال حاضر آنها را معامله می‌کند، از جمله هرگونه برنامه ریزی یا ملحقات احتمالی

برای دارایی‌های دیجیتال که در حال حاضر نگهداری می‌شود از مدیریت پرس و جو کنید. نمونه‌هایی از این ملاحظات شامل شناسایی و نظارت بر اشخاص وابسته و توانایی اثبات مالکیت است. ماهیت و گستردگی دفاتر، اسناد و مدارک برای پشتیبانی ادعاهای مدیریت در صورتهای مالی ممکن است به دارایی‌های دیجیتال خاصی بستگی داشته باشد.

- ♦ در صورت لزوم، در مورد مواردی که به حسابرس کمک می‌کند تا تصمیم بگیرد که آیا این قرارداد را قبول کند یا خیر، مطابق با بند ۱۱۰ از بخش ۲۱۰ AU-C ۱۴، از حسابرس قبلی پرس و جو کنید.
- ♦ برای آگاهی از اینکه آیا مدیریت از اشخاص ثالث (به عنوان مثال متصدیان سرمایه گذاری یا صرافی‌ها) استفاده می‌کند و آیا گزارش مناسب SOC<sup>۱۵</sup> موجود است، از مدیریت پرس و جو کنید. اگر خدمات ارائه شده توسط ارائه دهندگان، مربوط به حسابرسی صورت های مالی واحد تجاری استفاده کننده باشد، علاوه بر کسب کردن و ارزیابی گزارش SOC، کسب شناخت از فرآیندها و کنترل‌های مدیریت نیز مرتبط خواهد بود. اگر احتمالاً گزارش SOC موجود نیست، در مورد روش‌های جایگزین انجام شده از مدیریت پرس و جو کنید. به عنوان مثال، اگر واحد تجاری از شخص ثالثی به عنوان متصدی نگهداری دارایی‌های دیجیتال خود استفاده می‌کند، از مدیریت پرس و جو کنید که آیا شخص ثالث دارایی‌های دیجیتال واحد تجاری را در یک آدرس عمومی جمع می‌کند که دارایی‌های دیجیتال دیگر سپرده-گذاران را نیز شامل می‌شود. وقتی متصدیان نگهداری دارایی‌های دیجیتال یکپارچه می‌شوند، مشتری ممکن است مانده حساب شخصی خود را برای هر دارایی دیجیتال از طریق رابط وب شخص ثالث ببیند، اما اینکه این دارایی‌های دیجیتالی در بلاکچین وجود داشته باشد، ممکن است برای مشتری شفاف نباشد. بعلاوه، اگر معاملات (خرید / فروش یا ارسال / دریافت) بین دو مشتری باشد که هر دو از همان واحد تجاری به عنوان متصدیان نگهداری استفاده می‌کنند، متصدی نگهداری ممکن است تصمیم بگیرد که وجوه را فقط در سیستم‌های داخلی خود منتقل کند تا اینکه از بلاکچین عمومی استفاده کند. هنگامی که دارایی‌ها در هم یکپارچه می‌شوند، ممکن است نگهداری دفاتر، اسناد و مدارک کافی و به دست آوردن شواهد حسابرسی مناسب و کافی برای مدیریت چالش‌برانگیزتر باشد. در شرایطی که درهم آمیختگی وجود دارد، برای حسابرسان مهم است که در مورد فرایندها و کنترل‌های مدیریت برای تایید

<sup>۱۴</sup> استاندارد حسابرسی ۲۱۰ ایران قرارداد حسابرسی

<sup>۱۵</sup> کنترل‌های سیستم و سازمان (SOC) مجموعه خدمات پیشنهادی CPA است که ممکن است در ارتباط با کنترل در سطح سیستم یک سازمان خدماتی یا کنترل‌های سطح واحد تجاری از سازمان‌های دیگر ارائه شود. گزارش‌های SOC ۱ بر کنترل‌های موجود در یک سازمان خدماتی مربوط به کنترل داخلی واحدهای تجاری استفاده کننده بر گزارشگری مالی و گزارش‌های SOC ۲ بر کنترل‌های یک سازمان خدماتی مربوط به امنیت، در دسترس بودن، یکپارچگی پردازش، رازداری و حریم خصوصی متمرکز است.

وجود دارایی‌های دیجیتال و حقوق واحد تجاری نسبت به آنها، قبل از پذیرش یا ادامه آن شناخت پیدا کنند. این احتمالاً شامل شناخت درباره این موضوع خواهد بود که آیا یک گزارش SOC مناسب برای شخص ثالثی که متصدی نگهداری دارایی‌های دیجیتال واحد تجاری و کنترل‌های واحد تجاری استفاده کننده مکمل است، موجود است یا اینکه اگر گزارش SOC موجود نباشد، روش‌های جایگزین را می‌توان انجام داد.

♦ برای شرکت‌هایی که عرضه اولیه ارز یا سازوکارهای مشابه برای ایجاد و توزیع دارایی‌های دیجیتال به دیگران را دارند یا قصد انجام آن را دارند، هدف تجاری این عرضه (به عنوان مثال، توکنیزاسیون سود یک مشارکت محدود در یک صندوق سرمایه‌گذاری دارای ریسک یا افزایش سرمایه برای توسعه پلت فرم ابزاری) و ارزیابی تعهدات مدیریت، فرآیندها، تشخیص دادن، به روز ماندن و پیروی از قوانین و مقررات قابل اجرا (به عنوان مثال، ایالتی، محلی، فدرال و بین‌المللی) در این زمینه را بشناسید. افزایش گستره پرس و جوها از مشاور حقوقی واحد تجاری و بازرسی اسناد یا مکاتبات اضافی را در نظر بگیرید.

♦ برای شرکت‌هایی که می‌خواهند در یک عرضه اولیه ارز یا عرضه مشابه سرمایه‌گذاری کنند، فرآیند مدیریت را برای ارزیابی اینکه دارایی دیجیتال به عنوان یک اوراق بهادار<sup>۱۶</sup> محسوب می‌شود، از جمله استفاده از خبرگان مدیریت، رویه‌های مراقبت‌های لازم که واحد تجاری نسبت به طرف معامله انجام می‌دهد، منطق تجاری برای سرمایه‌گذاری در عرضه اولیه ارز و هدف تجاری طرف معامله از عرضه اولیه ارز را بشناسید.

♦ اطلاعات متناقضی را که با جستجو در رسانه‌ها و یا از منابع دیگر به دست آمده است، از جمله اطلاعاتی که از بررسی سابقه مدیریت و معیارهایی که ممکن است نشان دهنده اخلاقی نبودن مدیریت باشد را در نظر بگیرید.

<sup>۱۶</sup> کارمندان "SEC FinHub چارچوبی برای تجزیه و تحلیل دارایی‌های دیجیتال" قرارداد سرمایه‌گذاری "(۳ آوریل ۲۰۱۹)، چارچوبی را برای تجزیه و تحلیل اینکه دارایی دیجیتال به عنوان قرارداد سرمایه‌گذاری عرضه یا فروخته می‌شود، فراهم می‌کنند.



## ۵- فرآیندها، کنترل‌ها، از جمله فناوری اطلاعات

### استانداردهای حرفه ای مرتبط

همانطور که در بند ۰۶ بخش ۲۱۰-AU-C ۱۷ شرح داده شده است، پیش شرط حسابرسی، توانایی مدیریت در تهیه و به عهده گرفتن مسئولیت ارائه منصفانه صورت‌های مالی و طراحی، اجرا و نگهداری کنترل‌های داخلی موثر بر گزارشگری مالی است. میزان ارزیابی حسابرسان از این پیش شرط‌ها در فرآیند پذیرش و ادامه کار با صاحبکار، ممکن است به طور قابل توجهی متفاوت باشد. کار حسابرسی در اکوسیستم دارایی دیجیتال، اغلب پرس و جو دقیقی را در فرآیند پذیرش و ادامه کار با صاحبکار، برای ارزیابی این پیش شرط‌ها ایجاب می‌کند. این موضوع عمدتاً به دلیل پیچیدگی فناوری زیربنایی و ریسک‌های منحصر به فرد و چالش‌های مربوط به حسابرسی در جمع‌آوری شواهد حسابرسی مناسب و کافی است. کنترل‌های داخلی، از جمله کنترل فناوری اطلاعات، تأثیر مستقیمی بر قابلیت کنترل فعالیت مالی اساسی دارد و ممکن است لازم باشد حسابرسان برای درک این چالش‌ها، روش‌های سنتی پذیرش یا ادامه کار را گسترش دهند. به عنوان مثال، شناخت اینکه چگونه واحد تجاری به IT وابسته است و یا چگونه توسط آن قابل اجرا می‌شود و نحوه استفاده از سیستم‌های اطلاعاتی برای ثبت و نگهداری اطلاعات مالی ممکن است در فرآیند پذیرش یا ادامه کار با صاحبکار برای واحدهای تجاری که درگیر فناوری جدیدتری هستند، حیاتی‌تر باشد.

### چالش‌های خاص دارایی‌های دیجیتال

#### مرور کلی

کسب شناخت مناسب از نحوه استفاده واحد تجاری از دارایی‌های دیجیتال، زمینه زیربنایی IT و کنترل‌های اعمال شده توسط واحد تجاری بر دارایی‌های دیجیتال، احتمالاً برای حسابرس در تصمیم‌گیری در مورد پذیرش یا ادامه کار حسابرسی مربوط خواهد بود. در برخی موارد، حسابرس ممکن است پس از تصمیم اولیه پذیرش یا ادامه کار، با شرایطی روبرو شود که ممکن است دلیلی برای ارزیابی مجدد تصمیم باشد، مانند مواردی که حسابرس تشخیص داده است که مدیریت مسئولیت‌های خود در زمینه تهیه و ارائه منصفانه صورت‌های مالی را ایفا نکرده یا قادر به انجام آن نیست. به عنوان مثال، اگر واحد تجاری برای اولین بار معاملات دارایی‌های دیجیتال بااهمیتی را انجام داده باشد یا به طور استراتژیک به کسب و کاری بپردازد که از دارایی‌های دیجیتال در عملیات روزمره استفاده می‌کند،

<sup>۱۷</sup> استاندارد حسابرسی ۲۱۰ ایران قرارداد حسابرسی

مدیریت ممکن است از مجموعه مهارت و شناخت مناسب، دفاتر و اسناد و مدارک مثبت، یا کنترل‌های داخلی برای حسابداری و ارائه منصفانه دارایی‌های دیجیتال یا معاملات مرتبط در صورت‌های مالی، برخوردار نباشد.

برخی از کاربردهای فناوری بلاکچین می‌تواند نیاز به یک واسطه مرکزی (به عنوان مثال بانک‌ها) برای تکمیل معاملات را از بین ببرد. به همین ترتیب، شواهد حسابرسی که به طور سنتی از این واسطه‌ها در مورد وجود و حقوق و تعهدات دارایی به دست می‌آیند، در دسترس نیستند. اگر واحد تجاری دسترسی به کلید خصوصی را از دست بدهد، یا طرف دیگری به طور نامناسب به کلید خصوصی دسترسی پیدا کند و دارایی‌های دیجیتال را به آدرس عمومی دیگری منتقل کند در صورتی که واحد تجاری از کلید خصوصی اطلاع ندارد، در این صورت ممکن است واحد اقتصادی کنترل یا دسترسی به دارایی‌های دیجیتال را از دست بدهد. با توجه به این ویژگی‌ها، اطلاع از کلید خصوصی نشان دهنده کنترل دارایی‌های دیجیتال است. اگرچه ممکن است رویه‌هایی (به عنوان مثال، ارسال پیام‌های امضا شده یا انتقال دارایی‌ها) برای کنترل شواهد دارایی دیجیتال انجام شود، اما برای دستیابی به شواهد حسابرسی مناسب و کافی از مالکیت دارایی‌های دیجیتال توسط واحد تجاری (به طور مثال، آزمون اثربخشی عملیاتی کنترل‌ها بر مدیریت کلید خصوصی)، ممکن است اقدامات بیشتری انجام شود.

اگرچه گاهی ادعا می‌شود که فناوری بلاکچین نیاز به اعتماد را در بین شرکت‌کنندگان در معاملات از بین می‌برد، اما فناوری زیربنایی، اطلاعات موجود در آن را ذاتاً قابل اعتماد نمی‌کند. وقایع ثبت شده در بلاکچین کاملاً دقیق و کامل نیستند و قابلیت اطمینان داده‌های به دست آمده از بلاکچین بستگی زیادی به قابلیت اطمینان فناوری پیچیده زیربنای بلاکچین دارد. علاوه بر این، واحد تجاری ممکن است برنامه‌های جدید IT را که بین بلاکچین و سیستم گزارشگری مالی رابط دارند، پیاده‌سازی کنند. معرفی یک سیستم رابط ممکن است پیچیدگی محیط IT واحد تجاری را بیشتر کند.

ناشناس بودن هویت در بلاکچین عمومی اغلب ریسک‌های مربوط به معاملات اشخاص وابسته افشا نشده یا معاملات با واحدهای تجاری مشمول تحریم یا سایر مقررات را افزایش می‌دهد. آنها ممکن است در مورد معاملات مربوط به هم سوابقی نگهداری نکنند، در صورت وجود توافق طرف قرارداد اولیه، ممکن است چنین باشد. علاوه بر این، اگرچه دفتر کل بلاکچین ممکن است آدرس عمومی طرفین معامله کننده و مقدار ارز مبادله شده را ارائه کند و معاملات را بتوان با استفاده از شماره شناسایی معامله یا یک آدرس ردیابی کرد، اما این فناوری هیچ اطلاعاتی در مورد هویت طرف مقابل یا شناخت یا طبقه بندی مناسب در صورت‌های مالی ارائه نمی‌دهد.

در نتیجه این عوامل، ممکن است لازم باشد که حسابرس اثر بخشی برخی فرآیندها و کنترل‌ها را در زمینه دارایی-های دیجیتال بررسی کند زیرا ممکن است آزمون‌های محتوا به تنهایی برای به دست آوردن شواهد حسابرسی مناسب و کافی، کفایت نکنند.<sup>۱۸</sup> ( توجه: اگر حسابرس قصد دارد به کنترل‌ها اتکا کند، وی موظف است آن کنترل‌ها را بررسی کند.<sup>۱۹</sup> ) در نتیجه، پرس و جوهای دقیق تر یا بررسی اسناد مربوط در مورد کنترل داخلی سازمان و محیط IT ممکن است در فرآیند پذیرش و ادامه کار با صاحبکار مناسب باشد. چنین پرس و جو و بررسی ممکن است در زمینه های زیر متمرکز باشد:

- ♦ تکنولوژی و فناوری بلاکچین که توسط واحد تجاری برای ردیابی، انباشت، مغایرت‌گیری و گزارش مانده و معاملات دارایی‌های دیجیتال مورد استفاده قرار گرفته و به آن اعتماد کرده است.
- ♦ روش‌ها و کنترل‌های واحد تجاری که برای نگهداری و ایمن‌سازی دارایی‌های دیجیتال و تأیید و ردیابی معاملات دارایی دیجیتال اجرا شده است.
- ♦ کنترل‌های واحد تجاری که برای شناسایی، تأیید و تصویب اشخاص وابسته و روابط و معاملات با اشخاص وابسته ایجاد شده است.

در ادامه هر یک از این موضوعات با جزئیات بیشتری مورد بحث قرار گرفته است.

**تکنولوژی و فناوری بلاکچین که توسط واحد تجاری برای ردیابی، انباشت، مغایرت‌گیری و گزارش مانده و معاملات دارایی‌های دیجیتال مورد استفاده قرار گرفته و به آن اعتماد کرده است.**

در طی فرآیند پذیرش و ادامه کار با صاحبکار، دستیابی به شناختی از ماهیت فناوری بلاکچین و فناوری مورد استفاده برای ردیابی، انباشت، مغایرت‌گیری و گزارش مانده و معاملات دارایی‌های دیجیتال به حسابرس کمک می‌کند تا میزان روش‌های حسابرسی مورد نیاز را ارزیابی کند. ماهیت و میزان روش‌های انجام شده برای به دست آوردن شناختی از فناوری مورد استفاده توسط واحد تجاری، بسته به نقش واحد تجاری در اکوسیستم دارایی دیجیتال متفاوت خواهد بود.

برای حسابرس مهم است که شناخت درستی از فناوری زیربنایی بلاکچین مربوط به معاملات دارایی دیجیتال داشته باشد. اگر واحد تجاری دفاتر و اسناد و مدارک و معاملات خود را تنها از بلاکچین یا اظهارات ارائه شده توسط

<sup>۱۸</sup> بند ۳۱ بخش AU-C.۳۱۵ ( بند ۳۰ استاندارد حسابرسی ۳۱۵ ایران، تشخیص و ارزیابی خطرهای تحریف بااهمیت از طریق شناخت واحد تجاری و محیط آن).

<sup>۱۹</sup> بند ۰۷ بخش AU-C.۳۳۰ ( بند ۸ استاندارد حسابرسی ۳۳۰ ایران، برخورد های حسابرس با خطرهای ارزیابی شده ).

شخص ثالث بدست آورد، حسابرس ممکن است، به عنوان بخشی از فرآیند پذیرش و ادامه کار، فرایندهای مدیریت و کنترل کیفیت این اطلاعات، بخواهد شناخت بیشتری داشته باشد. در موارد خاص، شواهد حسابرسی به دست آمده از بلاکچین یا چنین اشخاص ثالثی ممکن است شواهد حسابرسی مناسب و کافی نباشد، و اقدامات بعدی را ایجاب کند.

همانطور که بیان شد، واحدهای اقتصادی ممکن است جدا از بلاکچین یا شخص ثالث، سیستم‌های گزارشگری مالی جداگانه‌ای داشته باشند تا ارزیابی کنند که آیا معاملات دارایی دیجیتال را به طور مناسب در سوابق مالی خود ثبت نموده اند یا خیر. به عنوان مثال، مغایرت‌گیری مانده دارایی‌های دیجیتال و معاملات از اسناد و مدارک حسابداری تا بلاکچین مربوط یا شخص ثالث ممکن است از طریق فرایندهای دستی یا خودکار انجام شود.

حجم معاملات حسابداری و آدرس‌های پردازش شده توسط واحد تجاری و نحوه پردازش این مانده‌ها و معاملات، از جمله اینکه واحد تجاری کپی بلاکچین را برای مغایرت‌گیری مستقل معاملات حفظ می‌کند یا اینکه سیستم‌ها در داخل توسعه یافته‌اند یا از اشخاص ثالث خریداری شده‌اند، ممکن است برای تعیین میزان روش‌های حسابرسی لازم برای به دست آوردن شواهد حسابرسی مناسب و کافی نیز مهم باشد.

علاوه بر این، میزان ثبت مانده و معاملات توسط واحد تجاری و انتقال آن به بلاکچین نیز ممکن است مهم باشد. برخی از واحدهای تجاری، در درجه اول واحدهای تجاری که در مبادلات دارایی دیجیتال فعالیت می‌کنند، فقط در صورت انجام معامله بین آدرس کنترل شده و آدرس کنترل نشده توسط واحد تجاری، ممکن است معاملات مشتریان خود را در یک دفتر داخلی ثبت کنند و معاملات را برای ثبت در بلاکچین ارسال کنند. معاملات برون زنجیره‌ای ممکن است در مقایسه با معامله‌ای که در بلاکچین ثبت شده، چالش‌های دیگری در به دست آوردن شواهد حسابرسی ایجاد کند.

معاملات و محافظت از دارایی‌های دیجیتال معمولاً به تعدادی سیستم IT برای پردازش و ثبت فعالیت دارایی‌های دیجیتال نیاز دارد. به این ترتیب، حسابرس ممکن است ارزیابی کند که آیا آزمون‌های محتوا به تنهایی شواهد حسابرسی مناسب و کافی را ارائه می‌کنند. در مواردی که آزمون‌های محتوا به تنهایی شواهد حسابرسی مناسب و کافی را ارائه ندهند، به دست آوردن شناخت از طراحی، پیاده‌سازی و اثربخشی عملکرد کنترل‌های عمومی IT و کنترل‌های کاربردی، ممکن است در روند پذیرش یا ادامه کار با صاحبکار مهم باشد.

نهایتاً، با توجه به ماهیت تکامل یافته صنعت و فناوری مورد استفاده شرکت‌های فعال در اکوسیستم دارایی‌های دیجیتال، برای مدیریت و حسابرس مهم است که از تغییرات فعلی و پیش بینی شده فناوری پایه‌ای مورد استفاده واحد تجاری مطلع شوند.

## **روش‌ها و کنترل‌های واحد تجاری که برای نگهداری و امنیت دارایی‌های دیجیتال و تایید و ردیابی معاملات دارایی دیجیتال اجرا شده است.**

معاملات بلاکچین به گونه‌ای طراحی شده‌اند که برگشت دادن آنها دشوار یا غیرممکن است. اگرچه می‌توان برای هر برنامه سیستم ثبت حسابداری دوطرفه نیز همین را گفت، اما ماهیت هم‌تا به هم‌تای بلاکچین بدین معناست که هنگامی که واحد تجاری معامله‌ای را به آدرس کیف پول خاصی ارسال می‌کند، هیچ ثبت بلاکچین تعدیلی وجود ندارد که بتواند انجام شود مگر اینکه طرف مقابل به طور فعال درگیر شود. به همین ترتیب، انتقال دارایی‌های دیجیتالی اشتباه یا نامناسب ممکن است منجر به از بین رفتن دائمی دارایی‌های دیجیتالی شود. در نتیجه، کنترل بر شروع و مجوز معاملات بسیار مهم است.

به همین ترتیب، با توجه به اینکه دارایی‌های دیجیتالی با استفاده از رمزنگاری که منجر به "کلیدهای خصوصی" می‌شود که کنترل (یعنی توانایی انتقال) دارایی‌های دیجیتال مرتبط را تامین می‌کند، ایمن است، این یک خطر ذاتی است که می‌تواند کلیدهای خصوصی سرقت شود، یا توسط طرف‌های داخلی یا خارجی مورد سوء استفاده قرار بگیرد. یک نمونه از سوء استفاده می‌تواند اشتراک کلیدهای خصوصی برای تسهیل گزارش نادرست عمدی دارایی‌ها از طریق تقلب باشد. امنیت کلید خصوصی و شناخت چگونگی کنترل کلیدهای خصوصی از اهمیت زیادی برخوردار است، زیرا هر کسی که به کلیدهای خصوصی دارایی‌های واحد تجاری دسترسی داشته باشد می‌تواند از آن دارایی‌ها استفاده کند یا آنها را ارسال کند و بنابراین کسب شناخت از روش‌های واحد تجاری برای ذخیره و حفاظت از کلید خصوصی (به عنوان مثال، خود ذخیره سازی گرم/ سرد یا از طریق متصدی نگهداری ثالث) دارای اهمیت است.

## **دارایی‌های دیجیتال نگهداری شده توسط واحد تجاری**

اگر واحد تجاری خود دارایی‌های دیجیتالی را ذخیره کند، توانایی‌های فنی مربوط به واحد تجاری، از جمله توانایی واحد تجاری در تایید وجود دارایی دیجیتال و همچنین محافظت‌های لازم برای جلوگیری از بین رفتن دارایی دیجیتال به دلیل تقلب یا اشتباه ممکن است برای حسابرس مهم باشد.

کسب شناخت از محافظت‌های واحد تجاری مربوط به ذخیره سازی و شروع معامله و مجوز دارایی‌های دیجیتال، ممکن است شامل پرس و جو در مورد سیاست‌ها، فرایندها و کنترل‌های مربوط به موارد زیر باشد، اما محدود به آن نیست:

- ♦ امنیت موقعیت مکانی کلیدهای خصوصی
- ♦ فرآیندهای مربوط به مدیریت چرخه عمر کلید، از جمله فرآیند تولید کلید (سخت افزار، نرم افزار و الگوریتم‌های مرتبط با تولید)
- ♦ امنیت مراکز داده واحد تجاری
- ♦ دسترسی به کلیدهای خصوصی، از جمله کلیدهای خصوصی اضافی
- ♦ تعداد کاربران مورد نیاز برای پردازش یک معامله، چه از طریق رمزگذاری و تقسیم کلیدها یا الزامات قابلیت چند امضایی
- ♦ تفکیک وظایف در اعطای مجوز معاملات دارایی‌های دیجیتال

حسابرس باید شناختی از چگونگی مدیریت برای ارائه شواهد مربوط به ادعای مالکیت دارایی‌های دیجیتال بدست آورد. در برخی موارد، مدیریت ممکن است ادعا کند که توانایی واحد تجاری در امضای پیام‌ها (sign messages)، کنترل آنها بر این دارایی‌های دیجیتالی را نشان می‌دهد و بنابراین می‌تواند شواهد حسابرسی ادعای مالکیت را ارائه دهد. در موارد خاص، محدودیت‌های عملیاتی ممکن است شخص را از امضای پیام با استفاده از کلیدهای خصوصی خود منع کند، که این امر شواهد محتوایی موجود را برای حمایت از ادعای مالکیت بیشتر کاهش می‌دهد. اگرچه کنترل دارایی دیجیتال یکی از ملاحظات ارزیابی ادعای مالکیت است، اما حسابرس باید تعیین کند که آیا نشان دادن کنترل از این طریق، شواهد کافی از مالکیت دارایی‌های دیجیتال مربوط را نشان می‌دهد یا ملاحظات یا روش‌های دیگر، مانند آزمون اثربخشی کنترل‌های داخلی لازم است. حسابرس ممکن است تشخیص دهد که آزمون‌های محتوا به تنهایی برای ارائه شواهد حسابرسی کافی و مناسب از ادعای مالکیت کافی نیستند.

### دارایی‌های دیجیتال نگهداری شده توسط متصدی نگهداری ثالث

اگر واحد تجاری برای نگهداری دارایی‌های دیجیتال خود به متصدی نگهداری ثالثی اعتماد کند، حسابرس ریسک‌های اضافی را هم برای واحد تجاری و هم برای نگهدارنده در نظر می‌گیرد. تعیین سطح تعامل بین واحد تجاری و

متصدی نگهداری، از جمله افرادی که توانایی شروع معاملات را دارند، ممکن است برای تعیین وجود پیش شرط- های حسابرسی ضروری باشد. به عنوان مثال، روش‌های حسابرسی برای آزمون مالکیت دارایی دیجیتال از طریق به دست آوردن پیام‌های امضا شده ممکن است نیاز به تعامل با متصدی نگهداری داشته باشد. در این صورت، درک اینکه متصدی نگهداری مایل و از نظر فنی قادر به کمک در فرآیند حسابرسی است، به حسابرس برای ارزیابی اینکه آیا پیش شرط‌های حسابرسی وجود دارد، کمک می‌کند. همانطور که اشاره شد، برای تعیین اینکه آیا می‌توان شواهد حسابرسی مناسب و کافی را برای اثبات مالکیت دارایی دیجیتال مربوط بدست آورد، ممکن است به داوری حرفه‌ای نیاز باشد.

به دلیل امنیت، کارایی یا سایر دلایل، متصدی نگهداری ممکن است دارایی بسیاری از مشتریان را در آدرس‌های مشابه درهم آمیخته کند و دفتر را خارج از زنجیره خود نگه دارد. دفترهای مختلط (درهم آمیخته شده) و خارج از زنجیره می‌تواند تاییدیه حسابرس در مورد دارایی‌های خاص واحد تجاری را که توسط متصدی نگهداری می‌شود، پیچیده کند، زیرا بلاکچین دیگر فقط نماینده دارایی‌های واحد تجاری نیست. در این موارد، ممکن است لازم باشد حسابرس روش‌هایی را برای تاییدیه مانده (دارایی‌های دیجیتال) با متصدی نگهداری را در نظر بگیرد. روش‌های تاییدیه، حسابرس را ملزم می‌کند که تشخیص دهد آیا تاییدیه متصدی نگهدارنده به عنوان شواهد حسابرسی معتبر می‌باشد، که این هم ممکن است به روش‌های بیشتر نیاز داشته باشد. از زمان نگارش این مقاله، هیچ فرم تاییدیه یا فرآیند تاییدیه پذیرفته شده‌ای برای متصدیان نگهداری دارایی یا صرافی‌های دارایی دیجیتالی مشابه آنچه برای مانده‌های نقدی موجود در موسسات مالی وجود دارد، موجود نیست.

مدیریت، مسئولیت طراحی، اجرا و حفظ کنترل داخلی مربوط به تهیه و ارائه منصفانه صورت‌های مالی، از جمله ایجاد کنترل بر اطلاعات دریافت شده از سازمانهای خدماتی مانند مبادله یا کنترل محافظت از دارایی را که ممکن است نزد متصدی نگهداری ایجاد شود، بر عهده دارد. به عنوان بخشی از فرآیند پذیرش و ادامه کار، حسابرس ممکن است به دنبال شناخت کنترل‌های اعمال شده توسط مدیریت برای نظارت بر سازمان‌های خدماتی باشد. کنترل‌های مدیریت ممکن است شامل انجام بررسی‌های مناسب از گزارش‌های SOC توسط پرسنلی با مجموعه مهارت و صلاحیت مرتبط و اجرای کنترل‌های مکمل باشد. در صورت در دسترس نبودن گزارش‌های SOC، شناخت کنترل‌های جایگزین اعمال شده توسط مدیریت (به عنوان مثال مغایرت‌گیری داده‌های شخص ثالث با دفاتر، اسناد و مدارک مستقل واحد تجاری) مهم خواهد بود. حسابرس ممکن است بخواهد گزارش SOC را بدست آورد تا بررسی کند که آیا حسابرس می‌تواند به عنوان بخشی از فرآیند پذیرش و ادامه کار به گزارش SOC اعتماد کند. اگر حسابرس نتواند تشخیص دهد که می‌تواند به گزارش SOC اعتماد کند یا دامنه گزارش برای اهداف

حسابرسی مربوط نیست، پرس و جو از صاحبکار در مورد توانایی حسابرس در انجام روش‌های حسابرسی در سازمان خدماتی به حسابرس کمک می‌کند تا کفایت شواهد حسابرسی را که می‌تواند بدست آورد را ارزیابی کند. غالباً متصدیان نگهداری به جای گزارش‌های ۱ SOC، گزارش‌های ۲ SOC را ارائه می‌دهند. اگرچه گزارش‌های ۲ SOC می‌توانند بینش بیشتری در مورد کنترل‌های اجرا شده برای پرداختن به اصول خدمات اطمینان‌دهی ارائه دهند، اما لزوماً بینشی درباره کنترل پردازش معاملات برای گزارش صورت‌های مالی ارائه نمی‌دهند. علاوه بر این، گزارش‌های ۱ SOC ممکن است حاوی اهداف کنترلی مربوط به تولید، ایمنی و نظارت بر کلیدهای مورد استفاده در این معاملات نباشد، و کمبود این اطلاعات ممکن است در به دست آوردن شناخت کاملی از کنترل‌های مربوط به گزارشگری مالی تاثیر بگذارد. اگر گزارش SOC در دسترس نباشد، برای حسابرس مهم است که بررسی کند آیا روش‌های بیشتر برای دستیابی به شواهد حسابرسی مناسب و کافی برای اتکا به اطلاعات ایجاد شده توسط سازمان خدماتی لازم و عملی است.

علاوه بر این، به دلیل ناشناس بودن هویت در معاملات بلاکچین، به دست آوردن شناخت از مشتریان و روش‌های دقت عمل که توسط متصدی نگهداری انجام می‌شود، به حسابرس کمک می‌کند تا تعیین کند که آیا مخاطرات تجاری در ارتباط با متصدی نگهداری می‌تواند منجر به مخاطرات قانونی یا سایر ریسک‌های مرتبط با عدم رعایت قوانین بانکی یا پولشویی یا سایر مقررات شود.

### **کنترل‌های واحد تجاری که برای شناسایی، تایید و تصویب اشخاص وابسته و روابط و معاملات با اشخاص وابسته ایجاد شده است**

ماهیت ناشناس بودن هویت در معاملات بلاکچین ممکن است چالش‌هایی را در تعیین هویت طرف‌هایی که واحد تجاری با آنها معامله می‌کند ایجاد کند، از این رو ریسک مرتبط با کامل بودن، معاملات و افشای اشخاص وابسته را افزایش می‌دهد. شناخت سیاست‌ها، فرایندها و کنترل‌های انجام شده توسط واحد تجاری، حسابرس را در ارزیابی ریسک شخص مقابل در معاملات واحد تجاری به عنوان یک شخص وابسته بالقوه افشا نشده یاری می‌کند.

پرس و جو حسابرس پیرامون انطباق با شناخت مشتری و قوانین پولشویی و سایر مقررات همانطور که در بخش ۴ به طور همزمان با سایر فرایندها بحث شده است، می‌تواند در شناسایی اشخاص و روابط وابسته و همچنین معاملات با اشخاص وابسته کمک کند.



## ملاحظات خاص روش‌های حسابرسی دارایی‌های دیجیتال

در بخش قبلی چالش‌ها و همچنین برخی از سوالات یا روش‌هایی را که ممکن است حساب‌برسان برای حل چالش‌های اساسی لحاظ کنند، در نظر گرفته شد. برخی از روش‌های بیشتر خاص برای اکوسیستم دارایی دیجیتال که به عنوان بخشی از فرآیند پذیرش و ادامه کار در نظر گرفته شده است، می‌تواند شامل موارد زیر باشد:

- ♦ برای شناخت ماهیت کنترل‌های عمومی IT، کنترل برنامه‌ها، فرایندهای موجود برای ردیابی، انباشت و مغایرت‌گیری دارایی‌های دیجیتال و همچنین کاهش مخاطرات IT مربوط به فناوری زیربنایی بلاکچین و هرگونه نارسایی‌های شناخته شده، از مدیریت، به ویژه کسانی که در بخش IT هستند، پرس و جو کنید.
- ♦ صلاحیت پرسنل واحد تجاری مرتبط با کنترل‌ها و فرآیندها را ارزیابی کنید و فناوری مورد استفاده برای معامله با دارایی‌های دیجیتال را بشناسید.
- ♦ نحوه استفاده واحد تجاری از کارشناسان فناوری اطلاعات (درون سازمانی یا برون سازمانی) و اینکه آیا برنامه‌هایی برای اجرای فناوری جدید برای پردازش معاملات دارایی دیجیتال وجود دارد را بشناسید. دارایی‌های دیجیتالی جدید که توسط فناوری‌های جدید ایجاد و پشتیبانی می‌شوند، نیاز به مدیریت دارند تا بتوانند فرایندهایی را برای خواندن و پردازش معاملات دارایی‌های دیجیتال و حساب کردن آنها پیاده سازی کنند.
- ♦ نحوه استفاده واحد تجاری از سازمان‌های خدماتی (به عنوان مثال، برای ایمن سازی کلیدهای خصوصی) و در دسترس بودن گزارش‌های SOC را در نظر بگیرید. هرگونه گزارش SOC (از جمله گزارش SOC ۲) موجود را بخوانید و درک کنید که آیا مدیریت کنترل‌هایی برای بررسی گزارش‌های SOC ۱ و کنترل‌های واحد تجاری استفاده کننده مکمل، دارد. حساب‌برس باید بر پاسخگویی کنترل‌های موجود در گزارش SOC در رابطه با مخاطرات گزارشگری مالی تمرکز کند.
- ♦ از مدیریت برای شناخت رویه‌های راستی‌آزمایی آنها که در رابطه با ارائه دهندگان خدمات شخص ثالث انجام می‌شود (به عنوان مثال متصدیان نگهداری)، از جمله شناخت فرآیندها و کنترل‌های انجام شده توسط شخص ثالث مربوط به معارفه و معاشرت سازمانی با مشتریان و راستی‌آزمایی، پرس و جو کنید.

♦ شناخت فرایند راستی آزمایی واحد تجاری برای معامله در دارایی‌های دیجیتال جدید، از قبیل نحوه ارزیابی دستورالعمل توافق عمومی، و مدل و فرآیند ارزیابی نرم افزار کیف پول موجود را که ممکن است برای معامله لازم باشد. در نظر بگیرید که آیا دارایی‌های خاصی که به طور ویژه برای افزایش بیشتر حریم خصوصی افراد طراحی شده اند، می‌توانند بر توانایی حسابرس در به دست آوردن شواهد حسابرسی کافی و مناسب تاثیرگذار باشند.

♦ محافظت واحد تجاری از کلیدهای خصوصی و سایر اطلاعات صاحبکار، از جمله موارد زیر را در نظر بگیرید:

- زیرساخت‌های مورد استفاده برای تولید و نگهداری کلیدهای خصوصی، از جمله نحوه نگهداری

کلیدهای خصوصی (به عنوان مثال کیف پول گرم و کیف پول سرد)

- تفکیک وظایف در اعطای مجوز معاملات دارایی‌های دیجیتال

- تعداد کاربران مورد نیاز برای پردازش یک معامله، چه از طریق رمزگذاری و تقسیم کلیدها یا

الزامات قابلیت چند امضایی

- نظارت بر آدرس‌ها برای هرگونه فعالیت غیر مجاز

♦ فرآیند واحد تجاری را برای تشخیص، حسابداری و افشای اشخاص و روابط وابسته، و همچنین معاملات اشخاص وابسته در نظر بگیرید.

♦ وجود جرایم اینترنتی یا بیمه سرقت از شرکت‌های مخابراتی معتبر را در نظر بگیرید.

♦ نرم افزار کیف پول و نسخه پشتیبان تهیه کیف پول را در نظر بگیرید (به عنوان مثال، اینکه آیا از

اطلاعات کلید خصوصی رمزنگاری شده پشتیبان تهیه می‌شود تا در صورت خرابی سیستم، دسترسی

مستمر به کلید خصوصی را برای واحد تجاری فراهم کند).



Association  
of International  
Certified Professional  
Accountants™

AICPA® CIMA®

The Association of International Certified Professional Accountants, powering leaders in accounting and finance around the globe

© 2020 Association of International Certified Professional Accountants. All rights reserved. AICPA and CIMA are trademarks of the American Institute of CPAs and The Chartered Institute of Management Accountants, respectively, and are registered in the US, the EU, the UK and other countries. The Globe Design is a trademark of the Association of International Certified Professional Accountants.

For information about the procedure for requesting permission to make copies of any part of this work, please email [copyright-permissions@aicpa-cima.com](mailto:copyright-permissions@aicpa-cima.com) with your request. Otherwise, requests should be written and mailed to Permissions Department, 220 Leigh Farm Road, Durham, NC 27707-8110 USA. 2010-83305