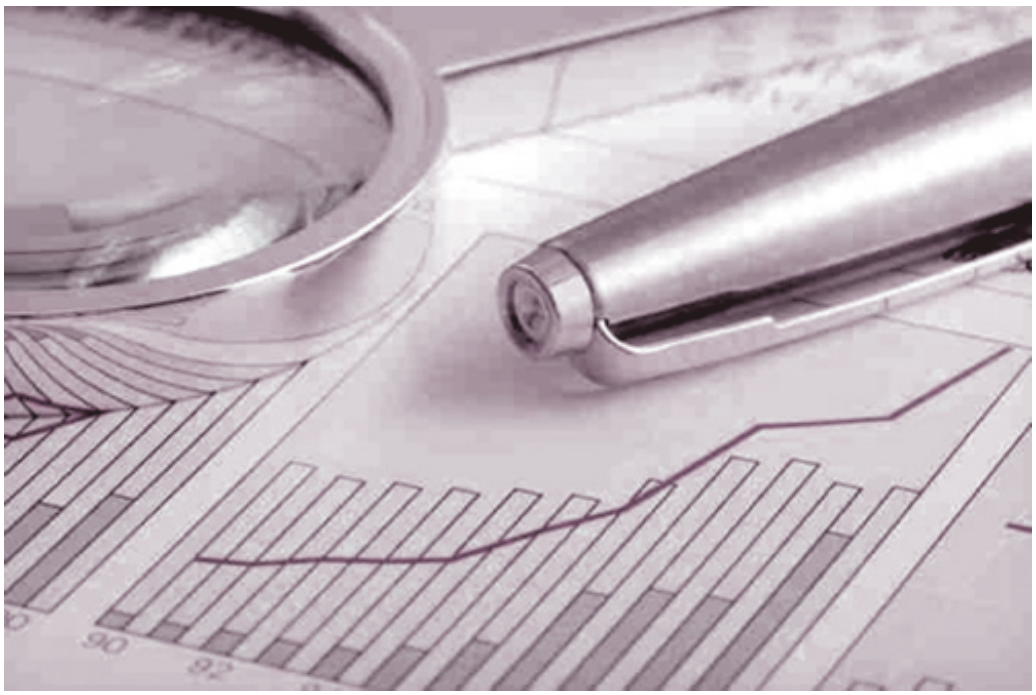


ارزیابی حسابرسان فناوری اطلاعات

ابراهیم ابراهیمی
موسی جوانی

مقدمه

تحول در محیط کسب‌وکار، متأثر از عواملی همچون محیط فناوری است. فناوری اطلاعات همیشه در قلب آنچه برای سازمان و سهامدارانش ارزش می‌آفریند، قرار می‌گیرد؛ یعنی دستیابی به چشم‌انداز و هدفهای سازمان به طریق کاراتر، اثربخش‌تر و به‌ویژه شفاف‌تر و قابل رسیدگی. بهترین روش برای اطمینان از این ارزش، حسابرسی و یا بررسی و ارزیابی فناوری اطلاعات است که تحقق این امر نیازمند پشتیبانی از نیازهای حسابرسی فناوری اطلاعات و ایجاد چارچوبی برای انجام آن است. زمانی که حسابرس فناوری اطلاعات مشغول انجام پروژه‌های اطمینان‌بخشی یا حسابرسی فناوری اطلاعات می‌شود، دستکم یک نفر آن کار را بررسی می‌کند. به‌طور کلی، حرفه حسابرسی ساختارها و فرایند هایی را توسعه داده تا اطمینان حاصل شود که حسابرسی و دیگر پروژه‌های مشابه، در معرض سطح مناسبی از بررسی پیش از انتشار آن است. این فرایندها بیشتر اوقات مستلزم چندین لایه بررسی است. هر چه ریسکهای مرتبط با پروژه‌ها بیشتر باشد، فرایندها به‌صورت دقیقتری بررسی شده و لایه‌های بیشتری از ساختارها را دربرمی‌گیرد.

فرایند بررسی از این‌رو طراحی شده است تا اطمینان دهد که محصول مورد انتظار متناسب با درخواست اولیه، نتایج آزمونها و رویه‌ها و متون فنی و رهنمودهای موضوع مورد بررسی است. برای انجام بررسی کیفیت، به سطحی از دانش و مهارت نیاز است. نکته اصلی این است که شخص دارای تخصص در حوزه موضوع مورد بررسی، به‌عنوان رهبر بررسی‌کننده خواهد بود.

بنابراین، در حوزه فناوری اطلاعات برای حسابرسی صورتهای مالی، بررسی‌کننده احتمال دارد شریکی باشد که درباره فناوری اطلاعات آگاهی داشته و از صاحبکار، متنهای فنی و رهنمودهای صاحبکار آگاه و در این کار دارای تجربه‌های چندساله است. باید به این نکته نیز توجه داشت که همه افراد مشارکت‌کننده در پروژه تمایل دارند بررسی کیفیت به‌صورت داخلی و قبل از انتشار گزارش انجام شود.

پرسشهایی که در مقاله به آنها خواهیم پرداخت، عبارتند از اینکه از حسابرس تازه‌کار فناوری اطلاعات در طول فرایند بررسی چه انتظاری باید داشت؟ بررسی‌کنندگان با چه چیزهایی سروکار دارند؟ چه چیزهایی باعث می‌شود که بررسی‌کننده پروژه را به‌منظور تغییر به تیم حسابرسی فناوری اطلاعات ارجاع دهد؟ چگونه حسابرسان فناوری اطلاعات می‌توانند اطمینان حاصل کنند که فرایند بررسی طبق برنامه اجرا می‌شود؟ چک‌لیست بررسی‌کننده چگونه خواهد بود؟

دامنه و ریسک

در انجام کار، تعیین دامنه به فرایند «تعریف دقیق حوزه‌ها و محدوده‌های کاری که باید مورد بررسی قرار گیرد»، اطلاق می‌شود. تعیین دامنه، اثر عمده‌ای بر اینکه آیا فعالیتهای رسیدگی هدفهای استفاده‌کنندگان از گزارش را محقق ساخته است یا نه، دارد. در تعیین دامنه کار، ارزیابی ریسک نیز یکی از عناصر کلیدی است. حسابرسان فناوری اطلاعات باید هم ریسکهای پذیرش کار و هم ریسکهایی را که ممکن است در برخورد با موضوعهای مورد بررسی ایجاد شوند، مدنظر قرار دهند. بنابراین، حسابرس فناوری اطلاعات باید دو نوع ریسک را مدنظر قرار دهد (ISACA, 2008):

- ریسک پذیرش کار خاص: حسابرس باید این موضوع را مدنظر قرار دهد که آیا ریسکهایی وجود دارد که مانع حسابرس از دستیابی به یک نتیجه‌گیری یا بیان نظر درباره موضوعی خاص شود؟ ریسکهایی که این ملاحظه را تحت‌تأثیر قرار می‌دهند، شامل زمانبندی، انتظارهای مدیریت و ویژگیهای عمومی صاحبکار یا پروژه می‌شود.
- ریسکهای موضوع مورد بررسی: این نوع ریسکها شامل ریسکهای مربوط به موضوع مورد بررسی است و برای حوزه‌های خاص تحت بررسی کاربرد دارد. این ریسکها ماهیت، حدود و زمانبندی کار و نیز میزان آزمونها را تعیین می‌کند. بنابراین اولین چیزی که باید درباره فرایند بررسی دانست این است که ساختار و فرایندها همبستگی بالایی با ریسک دارد. به این معنی که هر چه ریسکهای مرتبط با پروژه حسابرسی فناوری اطلاعات بالاتر باشد، سطح موشکافی در فرایند بررسی بیشتر خواهد بود و احتمال اینکه لایه‌های متعددی از فرایند بررسی اعمال شود، بیشتر است. بنابراین اگر پروژه‌ای به دلیلی (یا دلایلی) ریسکهای مرتبط زیادی داشته باشد، حسابرس فناوری اطلاعات به این نتیجه می‌رسد که پروژه باید به‌صورت دقیق و شاید تخصصی‌تر از دیگر موارد بررسی شود.

گاهی اوقات، نوع بنگاه هم حالتی مشابه بررسی موشکافانه بالا به وجود می‌آورد. حسابرسی مؤسسه‌های مالی، بنگاههای بزرگ (مثل شرکتهای سهامی عام) یا شرکتهایی که به فناوری اطلاعات وابستگی زیادی دارند، در بیشتر مواقع به بررسی بیشتری نیاز دارند.

سطح اهمیت مسائل دیگر نیز ممکن است منجر به بررسی بیشتر شود. در بیشتر مواقع (نه همیشه) حتی حسابرسان فناوری اطلاعات در سطح واحد تجاری نیز نیاز فزاینده‌ای به بررسی پروژه‌هایی که احتمال دارد آن فرایندها را دربرگیرد، احساس می‌کنند. اگر ریسک به‌طور نسبی بالا باشد، باید احتیاط بیشتری در آزمونها و رویه‌ها، مستندسازی و کاربرگها و ارائه و گزارشگری اعمال شود (Singleton, 2013).

حوزه‌های مربوط برای فناوری اطلاعات در بررسی

بررسی، ابعاد زیادی از پروژه حسابرسی را جدا از جنبه‌های مرتبط با فناوری اطلاعات پوشش می‌دهد. جنبه‌های کلی (غیرفناوری اطلاعات) شامل برنامه‌ریزی، تخصص فنی اعضای گروه، استقلال کافی، روش‌شناسی و استفاده از کار دیگران در بین دیگر جنبه‌ها می‌شود. حوزه‌ای از بررسی که می‌تواند به فناوری اطلاعات مربوط باشد، در بخشهای زیر شرح داده می‌شود.

مهارت و آموزش فنی

اعضای فناوری اطلاعات یک حسابرسی یا پروژه در موقع ارزیابی سطح مناسب خبرگی، تخصص و تواناییهای فنی موردنیاز برای پروژه خاص، با دیگر افراد یکسان در نظر گرفته می‌شوند. یکی از موارد تمایز، تعداد زیرمجموعه‌های موجود فناوری اطلاعات و گاهی ضرورت و وجود متخصصان در آن است. برای مثال، شرکتهای با اندازه متوسط می‌توانند تجارت الکترونیک را از طریق تارنما و با استفاده از یک سازمان خدماتی برای محافظت و پشتیبانی از پرداختها به‌کار گیرند. این سازمانها از خدمات ابری استفاده می‌کنند و گروهی دیگر از تأثیرگذاران مرتبط با فناوری اطلاعات را درگیر می‌کنند. این نیازهای فعلی برای حوزه‌های تخصصی و متعدد فناوری اطلاعات می‌تواند برای یک واحد تجاری مطرح شود.

مسئله دوم، ضرورت حفظ مهارت و توانایی کافی و به‌روز است. این مسئله بدون اشاره به عبارت «زمانی که یک شخص حرفه‌ای حسابرسی فناوری اطلاعات (یا هر حرفه دیگر فناوری اطلاعات) را انتخاب می‌کند، آن شخص به یادگیری مادام‌العمر متعهد می‌شود»، در حال گذر است. فناوری اطلاعات به‌سرعت در حال تغییر است و مهارت و توانایی فرد می‌تواند در عرض چند سال از رده خارج شود؛ بنابراین یک جنبه از ارزیابی ریسک فناوری اطلاعات در سطح واحد تجاری و شرکت، میزان پرورش و آموزشهای حرفه‌ای است که افراد هر ساله در سطح شرکت و فردی کسب می‌کنند. این مسائل در مورد حسابرسی فناوری اطلاعات نیز صادق است.

کنترلها: کنترلهای داخلی حاکم بر گزارشگری مالی

کنترلها همواره به‌عنوان بخشی از حسابرسی فناوری اطلاعات یا پروژه اطمینان‌بخشی هستند؛ اما بسته به ماهیت پروژه یا هدفهای حسابرسی، می‌توانند متفاوت باشند. بنابراین هریک از جنبه‌های کنترلی که در ادامه خواهد آمد، ممکن است برای یک حسابرسی خاص کاربرد داشته باشد یا نداشته باشد. وقتی پروژه حسابرسی شامل گزارشگری مالی نیز هست، کنترلهای داخلی حاکم بر گزارشگری مالی جزء اصلی خواهد بود که بررسی‌کننده به‌دنبال آزمون آن است. بنابراین، حسابرس فناوری اطلاعات باید در حسابرسی صورتهای مالی مراقب باشد تا کنترلهای مرتبط با فناوری اطلاعات را برای کنترلهای داخلی حاکم بر گزارشگری مالی شناسایی کرده و اطمینان پیدا کند که درک مناسبی از برنامه‌های کاربردی، معاملات و ساختارهای مؤثر بر ارقام مالی به‌دست آمده است.

نمونه‌ای از یک چک‌لیست، برای بررسی این اقلام از سوی بررسی‌کننده در **نمایه ۱** ارائه شده است. البته باید اشاره داشت که چک‌لیست ارائه‌شده در اینجا براساس چک‌لیست مورد استفاده در حسابرسی مالی است. بنابراین، ممکن است تا حدی برای حسابرسی داخلی فناوری اطلاعات (کنترلهای کاربردی)، ساختار حسابرسی متفاوت باشد؛ اما اصول آنها یکی است.

اقلام ارائه‌شده در **نمایه ۱** باید طبق رهنمودهای معتبر و کاربرگها باشد. این کار نسبت به رعایت استانداردها و تعیین دامنه مناسب اقلام چک‌لیست اطمینان داده و فرایند بررسی را تسهیل می‌کند.

نمایه ۱ - نمونه چک‌لیست بررسی‌کننده در کنترلهای داخلی حاکم بر گزارشگری مالی

آیا تیم حسابرسی فناوری اطلاعات از موارد زیر شناخت کسب کرده است:

* برنامه‌های کاربردی که فرایندهای بااهمیت و طبقه‌های عمده معاملات عمده را پشتیبانی می‌کنند (برای مثال آیا نرم‌افزارها فرایند سپرده و واریز را پشتیبانی می‌کنند؟)
* معاملات چگونه در درون برنامه‌های کاربردی گردش دارند (برای مثال، معاملات چگونه شروع، تصویب، ثبت، پردازش و گزارش می‌شوند؟)
* آیا ساختارهای زیربنایی (مانند شبکه و سرورهای میزبان) برنامه‌های کاربردی شناسایی‌شده را پشتیبانی می‌کنند؟
* آیا تیم حسابرسی فناوری اطلاعات محیط کنترلی، ارزیابی ریسک و فعالیتهای پایشگری را ارزیابی کرده است؟

مستندسازی حسابرسی:

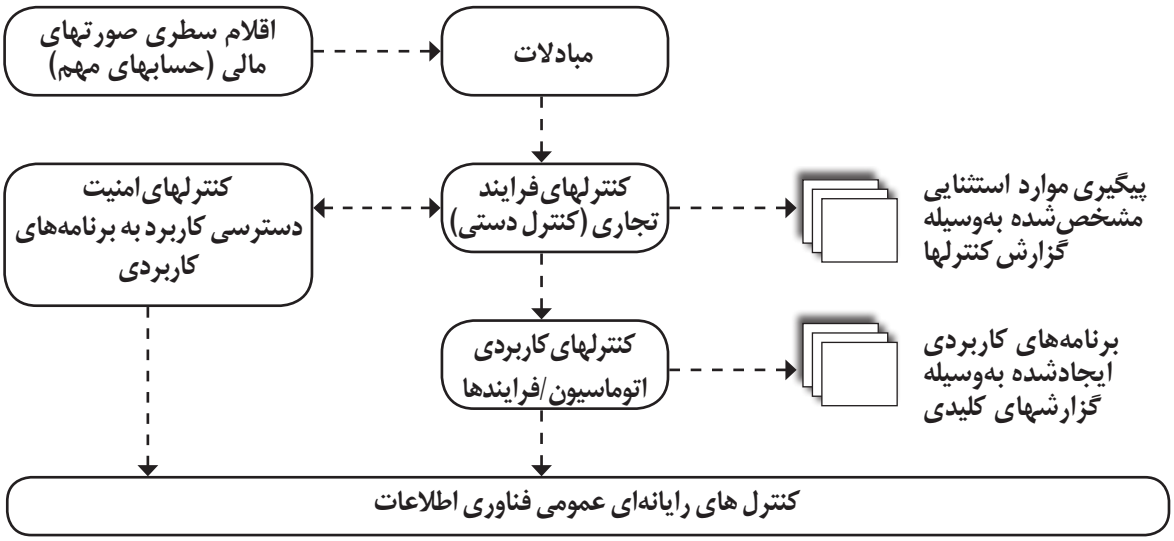
آیا شناخت از محیط فناوری اطلاعات مستند شده و در بخش برنامه‌ریزی کاربرگها نگهداری شده است؟

* آیا گروه حسابرسی فناوری اطلاعات محیط کنترلی، ارزیابی ریسک و فعالیتهای پایشگری را مستندسازی کرده است؟

کنترلها: در سطح بنگاه

جنبه دیگری از کنترلهای داخلی که بر کار حسابرسان فناوری اطلاعات اثرگذار است، کنترلهای داخلی در سطح بنگاه است. این کنترلها در سطح بالاتر بنگاه هستند و می‌توانند هدفهای

نمایه شماره ۳ – کنترل های عمومی فناوری اطلاعات و حسابرسی



حسابرسی فناوری اطلاعات یا پروژه را تحت‌تأثیر قرار دهند. کنترلهای یادشده دربرگیرنده کنترلهای مرتبط با هیئت‌مدیره (مانند راهبری فناوری اطلاعات)، کنترلهای مرتبط با مدیران اجرایی (مدیر فناوری اطلاعات) و دیگر کنترلهای فراگیر (گسترده) در سطح بنگاه است.

نمایه ۲- چک‌لیست نمونه بررسی‌کننده برای کنترلهای داخلی در سطح بنگاه

آیا گروه حسابرسی فناوری اطلاعات، محیط کنترلی فناوری اطلاعات صاحبکار را ارزیابی کرده است؟

مستندسازی حسابرسی:

آیا مستندسازی حسابرسی، پرسشنامه تکمیل‌شده مربوط به کنترلهای سطح بنگاه، و اطلاعات پشتیبان شامل شناخت سیستم را دربرمی‌گیرد؟

چک‌لیست بررسی‌کننده برای کنترلهای سطح بنگاه باید شبیه چک‌لیست ارائه‌شده در **نمایه ۲** باشد. بار دیگر یادآوری می‌کنیم اقلام ارائه‌شده در چک‌لیست به‌طور معمول مطابق کاربرگها و رهنمودهای معتبر است. اغلب (یا بیشتر اوقات)، تحلیل کنترلهای سطح بنگاه نیاز به بررسی کل فرایندهای آن خواهد داشت تا مشخص شود که آیا این کنترلها به‌صورت مناسب طراحی شده و اعمال می‌شوند یا نه. آزمون این کنترلها ممکن است در مراحل بعدی حسابرسی فناوری اطلاعات به‌لحاظ نظری ضروری باشد؛ اما گاهی اوقات به‌صورت همزمان و با شناسایی و تجزیه‌وتحلیل مستقیم انجام می‌شود.

کنترلها: کنترلهای عمومی فناوری اطلاعات

همزمان با استفاده از فناوری اطلاعات یکپارچه در سازمان، مباحثی مانند ارزیابی کنترلهای اعمالی بر برنامه‌های کاربردی کلیدی و کنترلهای حاکم بر امنیت دسترسی به داده‌ها و به‌طور کلی کنترلهای عمومی فناوری اطلاعات مطرح می‌شود. کنترلهای عمومی فناوری اطلاعات یکی از موضوعهای موردبحث روز در فناوری اطلاعات و کنترلها طی چند سال اخیر بوده است. کنترلهای عمومی فناوری اطلاعات بر حسابرسی صورتهای مالی، همه حسابرسی‌های داخلی فناوری اطلاعات، حسابرسی مستقل فناوری اطلاعات و راهبری فناوری اطلاعات مؤثر است. **نمایه ۳** به وضوح این اثر متقابل را نشان می‌دهد.

کنترلهای عمومی فناوری اطلاعات دارای چندین لایه است که هر کدام از آنها ریسکهای نسبی خود را دارند. این لایه‌ها عبارتند از:

نمایه ۴ - فهرست منابع معتبر برای کنترلهای عمومی فناوری اطلاعات

انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی چارچوب اطمینان‌بخشی فناوری اطلاعات	هیئت نظارت بر حسابداری شرکتهای سهامی عام **استاندارد حسابرسی شماره ۵** (PCAOB's AS۵)	**انجمن حسابداران رسمی امریکا** (AICPA) **مقاله حسابرسی فناوری اطلاعات** (AICPA's IT Audit White Paper)
* مقدمه‌ای بر کنترلهای عمومی فناوری اطلاعات * برنامه‌ریزی منابع اطلاعاتی * ارائه خدمات فناوری اطلاعات * عملیات سامانه‌های اطلاعاتی * منابع انسانی فناوری اطلاعات * برون‌سپاری و فعالیتهای شخص ثالث * مدیریت امنیت اطلاعات * چرخه عمر توسعه سامانه‌ها * برنامه‌ریزی مستمر کسب‌وکار و برنامه‌ریزی بازیابی * مدیریت پایگاه داده‌ها و کنترلها * پشتیبانی نرم‌افزار سامانه‌ها * کنترلها و مدیریت شبکه * پشتیبانی سخت‌افزار * کنترلها و مدیریت سیستم عملیات * کنترلهای فیزیکی و محیطی * درگاه‌های بنگاه * شناسایی و تأیید	* امنیت و دسترسی * عملیات رایانه‌ای * توسعه و تغییرهای سامانه	* محیط فناوری اطلاعات/ واحد فناوری اطلاعات * کنترلهای دسترسی * مدیریت تحول * برنامه‌ریزی مستمر بنگاه و برنامه‌ریزی بازیابی * کنترلهای برون‌سپاری/ سازمانهای خدماتی

لایه زیربنا[۱]: این لایه مربوط به زیرساختهای فناوری اطلاعات شرکت است.

لایه سرور میزبان[۲]: این لایه بیانگر سروروهای میزبان انجام خدمات فناوری اطلاعات است.

لایه برنامه‌های کاربردی[۳]: این لایه مربوط به برنامه‌های کاربردی مورد دسترسی کاربران است.

لایه دادگان[۴]: این لایه محل انبارش داده‌ها را نشان می‌دهد.

هرچه از لایه‌های زیربنایی به سمت لایه‌های دادگان حرکت کنیم، ریسک افزایش می‌یابد. فناوری اطلاعات و فرایند تجاری بنگاه به‌دنبال این هستند که این ریسکها را از طریق اعمال کنترلهای جبرانی و اضافی کاهش دهند (ابراهیمی، ۱۳۹۰).

یکی از مواردی که حسابرسان فناوری اطلاعات به‌عنوان مبنا به آن نیاز دارند، شناخت خوب از اجزای کنترلهای داخلی چگونگی اندازه‌گیری آنها، ریسک آنها و شیوه شناسایی کنترلها و ارزیابی اثربخشی آنها است. **انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی**[۵] چارچوبی را برای اطمینان از کیفیت، یکنواختی و اتکاپذیری ارزیابیهای فناوری اطلاعات موسوم به **چارچوب اطمینان‌بخشی فناوری اطلاعات**[۶] طراحی کرده است. این چارچوب منبع خوبی برای این قسمت می‌باشد.

چارچوب اطمینان‌بحشی، متمرکز بر منابع و استانداردهای انجمن راهبری فناوری اطلاعات و انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی و دیگر سازمانها است که منبعی واحد برای حسابرسی فناوری اطلاعات و افراد حرفه‌ای در این حوزه فراهم می‌سازد. این چارچوب ۱۷ حوزه کنترلهای عمومی فناوری اطلاعات را توصیف می‌کند.

هیئت نظارت بر حسابداری شرکتهای سهامی عام ۳۷ حوزه

نمایه ۵ -چک‌لیست نمونه بررسی‌کننده برای کنترلهای عمومی فناوری اطلاعات

آیا گروه حسابرسی فناوری اطلاعات کنترلهای عمومی فناوری اطلاعات را بررسی کرده است؟ آیا این بررسی ویژگیهای زیر را دربرگرفته است:

* شناسایی ریسک و هدفهای کنترلی مربوط
* شناسایی کنترلهای به‌جا و ارزیابی اثربخشی طراحی آنها
* شناخت کامل نقشه فرایندهای فناوری اطلاعات و کنترلهای موجود
* ویژگیهای آزمونهایی جهت ارزیابی کنترلهای شناسایی‌شده
* مستندسازی روشن نتایج آزمونهای انجام‌شده و ارزیابی اثربخشی عملیات
* کاربرگهای پشتیبان ارزیابی انجام‌شده
* ویژگیهای کاستیهای کنترلی و تجزیه‌وتحلیل اینکه آیا این کاستیها ممکن است منجر به ضعف بااهمیت و عمده در کنترلها شود.
* پیگیری رفع کاستیهای کنترلی از سوی مدیریت در کل سال(شامل آزمون ضعفهای کنترلی که در طی سال حسابرسی رفع شده است)
* آزمون پایان سال روشها

مستندسازی حسابرسی:

آیا مستندسازی حسابرسی:

* با جزئیات کافی تهیه شده است تا شناخت روشنی از هدفها، منابع و نتیجه‌گیری کسب‌شده آن ارائه کند؟
* با جزئیات کافی تهیه شده است تا درک روشنی درباره ماهیت، زمان‌بندی، میزان و نتایج رویه‌های انجام‌شده و شواهد کسب‌شده ارائه کند؟
* در شناسایی انواع آزمونها واضح هستند؟ (مانند بررسی و شرح کل فرایندها)
* در شناسایی مواردی مانند نمونه حسابرسی انتخاب‌شده از جامعه و منبع اندازه نمونه واضح است؟
* به‌صورت مناسب سازماندهی شده است تا ارتباط مناسبی به یافته‌ها یا مسائل بااهمیت ارائه کند؟
* قادر هست مشخص کند که چه کسی کار را انجام داده است؟ درچه تاریخی تکمیل شده است؟ سرپرست بررسی‌کننده چه کسی بوده ودر چه تاریخی بررسی صورت گرفته است؟

کنترلهای عمومی فناوری اطلاعات را توصیف می‌کند و در نهایت انجمن حسابداران رسمی امریکا ۵ حوزه را بیان می‌کند. در نمایه ۴ این حوزه‌ها ارائه شده است. به آسانی می‌توانیم این سه رده‌بندی را با یکدیگر تطبیق دهیم. بنابراین در اصل نسبت به کنترلهای عمومی فناوری اطلاعات توافق وجود دارد

نمایه -۶ چک‌لیست نمونه بررسی‌کننده برای کنترلهای کاربردی

آیا تیم حسابرسی و تیم حسابرسی فناوری اطلاعات به توافق می‌رسند که کنترلهای خودکار خاصی از نرم‌افزار کاربردی، به‌عنوان کنترل کلیدی هستند و تیم حسابرسی فناوری اطلاعات مسئولیت آزمون آن کنترل کلیدی را بر عهده گیرد؟

آیا تیم حسابرسی فناوری اطلاعات، آزمونهای مناسبی را برای کنترلهای عمومی فناوری اطلاعات حاکم بر نرم‌افزار کاربردی انجام می‌دهد؟ (همان‌طوری که در قبل اشاره شد، نرم‌افزار کاربردی شناسایی‌شده دربرگیرنده چند کنترل کلیدی خودکار است).

آیا تیم حسابرسی فناوری اطلاعات، آزمونهای مناسبی برای ارزیابی اثربخشی طراحی و اجرای کنترلهای خودکار شناسایی شده در نرم‌افزار کاربردی (شامل استفاده از نمونه مناسب که در تیم حسابرسی توافق شده است) انجام داده است؟

آیا تیم حسابرسی فناوری اطلاعات همکاری لازم را با تیم حسابرسی برای تکمیل تجزیه‌وتحلیل ضعفهای شناسایی‌شده در کنترلهای عمومی فناوری اطلاعات دارد؟

و تفاوت فقط در جزئیات هر یک از اقلام ارائه شده است.

حسابرسان فناوری اطلاعات باید بدانند که ضعف بااهمیت در کنترلهای عمومی فناوری اطلاعات، نه‌تنها این کنترلها بلکه دیگر کنترلها را نیز تحت‌تأثیر قرار می‌دهد. از دیدگاه **هیئت نظارت بر حسابداری شرکتهای سهامی عام**[۷]، کنترلهای عمومی فناوری اطلاعات کنترلهای در سطح بنگاه در نظر گرفته می‌شوند و بنابراین هرچیزی را در بخش فناوری اطلاعات و فراتر از آن در سامانه‌های اطلاعاتی، برنامه‌های کاربردی و فناوریهای دیگر تحت‌تأثیر قرار می‌دهند. به این دلیل است که رهنمودهای هیئت نظارت بر حسابداری شرکتهای سهامی عام و انجمن حسابداران رسمی امریکا بیان می‌کنند که اگر کنترلهای عمومی فناوری اطلاعات ضعف بااهمیتی داشته باشند، حسابرسان نمی‌توانند به کنترلهای کاربردی (که در واقع در سایه کنترلهای عمومی قرار گرفته‌اند) اتکا کنند.

چک‌لیست بررسی‌کننده برای کنترلهای عمومی فناوری

اطلاعات، شبیه چک‌لیست ارائه‌شده در **نمایه ۵** است که مطابق رهنمودهای معتبر و کاربرگهای مربوط است.

کنترلها: کاربردی

کنترلهای کاربردی بر حسب تعریف، کنترلهای خودکار یا کنترلهای مختلط (ترکیبی از کنترلهای خودکار و دستی) هستند. این کنترلها اطمینان می‌دهند که معاملات به‌صورت مناسبی شروع، تصویب، ثبت، پردازش و گزارش می‌شوند. هرچه قدر هدفهای کنترلی منتج شده از کنترلهای دستی بیشتر باشد، احتمال شکست کنترلها بیشتر است. همان‌طوری که متخصصان فناوری اطلاعات نیز می‌دانند، یک کنترل خودکار کامل، کار مشابهی را در طی زمان انجام می‌دهد. این کنترلها یک بار مورد آزمون قرار می‌گیرند و تا زمانی که فناوری یکپارچه تغییر نکند، نتایج مشابهی متناسب با هدف منظورشده تولید خواهند کرد.

حسابرسان فناوری اطلاعات باید بدانند که زمان مناسب برای به‌کارگیری کنترلهای کاربردی چه موقع است، چه کنترلهایی مربوط است، چگونه آنها را آزمون کنند، چگونه سطح اتکاپذیری آن و سطح اطمینان فراهم‌شده را ارزیابی کنند و چگونه آنها را با طرح کلی و برنامه حسابرسی متناسب کنند. بررسی‌کننده در پی چنین اطلاعاتی است.

چک‌لیست بررسی‌کننده برای کنترلهای عمومی، شبیه چک‌لیست ارائه‌شده در **نمایه ۶** است.

کاربرگها/ مستندسازی

همه حسابرسان می‌دانند که آزمونها و رویه‌های حسابرسی و دیگر جنبه‌های برنامه حسابرسی باید مستندسازی شود. محتویات کاربرگها به‌عنوان شواهد اصلی است که یافته‌ها و گزارش حسابرس را پشتیبانی می‌کند. افزون بر این، کاربرگها عامل کلیدی فرایند بررسی است. بررسی‌کننده به‌طور معمول از اطلاعاتی که روزانه جمع‌آوری می‌شود، آگاهی ندارد و طی فرایند حسابرسی به آن دسترسی ندارد. بنابراین بررسی‌کننده به بدنه اطلاعاتی وابسته است که باید استخراج و به‌طور کامل درک شود. به‌عنوان مثال، بداند چه کاری انجام شده، نتایج چه بوده، آیا آزمون و رویه‌های کافی انجام شده و آیا نتایج استخراج‌شده از بدنه اصلی شواهد،

حسابرسان فناوری اطلاعات باید هم ریسکهای پذیرش کار و هم ریسکهایی که ممکن است در برخورد با موضوعهای مورد بررسی ایجاد شوند را مدنظر قرار دهند

مناسب است؟ در حقیقت غیرعادی نیست که بررسی کننده (که به‌طور معمول یک سطح بالاتر از سرپرست گروه حسابرسی است) در اولین بررسی نسبت به برنامه حسابرسی سئوالی را مطرح کرده یا تعدیل شواهد و برنامه حسابرسی را درخواست کند. در چنین حالتی، انجام تعدیل از طریق دستور نوشتاری صورت می‌گیرد. وقتی این شرایط رخ می‌دهد، این فرایند به سرپرست گروه حسابرسی واگذار می‌شود تا خواسته‌های بررسی‌کننده را به‌صورت کامل شفاف‌سازی کند. بنابراین، کار دوباره به همان بررسی کننده ارجاع داده می‌شود. اثربخشی و کارایی این فرایند، تا اندازه زیادی به کیفیت کاربرگها، کامل بودن و شفافیت آنها به‌منظور درک استفاده کننده بستگی دارد.

گزارش

مورد آخر، گزارش است. گزارش بدون شک تابعی از بررسی است. گزارش باید مطابق با روش‌شناسی بنگاه و دیگر الزامهای فنی باشد. گزارش به احتمال زیاد مهمترین سندی است که بررسی می‌شود.

فرایند

فرایند کار تا حدودی توضیح داده شد؛ اما جریان آن به‌صورت زیر خواهد بود:

- رهبر گروه مستندسازی، کاربرگها و گزارش را قبل از ارسال آن به زنجیره بررسی، بررسی می‌کند.
- یک نفر از مافوقهای رهبر گروه، حسابرسی را مرور می‌کند. اگر مسئله یا مشکلی یافت شد، آن مسئله به رهبر گروه ارجاع

داده می‌شود.

- اغلب، افراد دیگری غیر از زنجیره بررسی به‌طور موازی، کار بررسی دوم را انجام می‌دهند.
- بسته به نوع حسابرسی (مانند ریسک) یا الزام بنگاه، ممکن است سومین بررسی نیز انجام شود.
- حتی اگر بخش داخلی کامل باشد، گاهی اوقات مؤسسه‌های خارجی فرایند بررسی و حسابرسی را بازرسی می‌کنند.

نتیجه‌گیری

اگر فرایند بررسی به‌طور مناسبی انجام شود، محصول به‌دست‌آمده، کیفیت کافی را خواهد داشت تا بتوان در برابر رسیدگی و تحلیل حامیان مالی و استفاده‌کنندگان مقاومت کند (این به معنای کیفیت حسابرسی است). بنابراین برای حسابرسان فناوری اطلاعات ارزشمند است که بدانند یک بررسی مناسب شامل چه اجزایی است، چگونه انجام می‌شود و چگونه می‌توان اطمینان یافت که این فرایند تا حد ممکن بدون مشکل باشد.

بررسی اغلب چند لایه است. رهبر گروه (مدیر)، گروه را بررسی می‌کند، شخص دیگری نیز (مانند شریک یا مدیر حسابرسی فناوری اطلاعات) کار رهبر گروه را بررسی می‌کند و لایه اضافی نیز ممکن است برای موقعیتهای خاص نیاز باشد. اما همه لایه‌های بررسی در کل به‌دنبال نتیجه مشابهی مانند موارد زیر هستند:

- دامنه مناسب در کل فرایند؛
- مستندسازی (کاربرگ) مناسب؛
- اینکه آیا پیکره کاربرگ نتایج را پشتیبانی می‌کند؛ و
- اینکه آیا گزارش به‌طور مناسب (از لحاظ قواعد نگارشی، تشریح مسائل به میزان کافی اما نه زیاد) نگارش شده تا به‌صورت اثربخش به هدفها توجه کند و آیا گزارش از لحاظ فنی صحیح است.

شاید بهترین رهنمود برای ارزیابی کار حسابرسان فناوری اطلاعات، همان چارچوب اطمینان‌بخشی فناوری اطلاعات باشد. این چارچوب دربرگیرنده اطلاعاتی درباره موضوعهای یادشده در این مقاله و بیشتر است. این چارچوب به‌ویژه می‌تواند فرایند بررسی را اثربخش و کاراتر سازد؛ زیرا حسابرسان فناوری اطلاعات قادرند کاری را در دامنه مربوط انجام دهند، شواهد کافی توسعه دهند، کنترلهای مناسب را در نظر بگیرند و نتیجه‌گیری مناسبی نیز اتخاذ کنند.

به‌منظور کمک به کارکرد مناسب فرایندها و جلوگیری از دور برگشت و توضیح مسائل برای بررسی‌کننده، حسابرسان فناوری اطلاعات باید در انجام وظایف خود کوشا باشند. به‌ویژه ضروری است آنها بعد از انجام کار، یک خودارزیابی داشته باشند و از خود بپرسند که:

- آیا همه هدفهای حسابرسی مورد توجه قرار گرفته است؟
- آیا آزمونها و رویه‌ها به اندازه کافی مناسب و قوی هستند که ریسکها را در برگیرند؟
- آیا همه قوانین و مقررات مرتبط در نظر گرفته شده است؟
- آیا بدنه شواهد به اندازه کافی هستند که یافته‌ها و نتیجه‌گیری‌ها را پشتیبانی کنند؟
- آیا کاربرگها به‌طور مناسبی با هدفهای حسابرسی و نتیجه‌گیری‌ها مرتبط هستند؟

چون بیشتر افراد تازه کار حسابرسی فناوری اطلاعات به تجربه و زمان کافی نیاز دارند تا رهنمودهای ارائه‌شده در اینجا را مورد توجه قرار دهند، حداقل باید آگاهی کسب کنند که چه کسی حسابرسان را حسابرسی می‌کند، چگونه این فرایند کار می‌کند و چگونه می‌توان این فرایند را کارا و اثربخش کرد.

پانوشتها:

1- Infrastructure
2- Host server
3- Application
4- Database
5- Information System Audit and Control Association (ISACA)
6- IT Assurance Framework (ITAF)
7- Public Company Accounting Oversight Board (PCAOB)

منابع:

- ابراهیمی ابراهیم، **نقش فناوری اطلاعات در پیشگیری یا کشف تقلب**، مجله حسابدار، شماره ۲۳۶، آبان ماه، ۱۳۹۰
- ISACA, **ITAFTM: A Professional Practices Framework for IT Assurance**, www.isaca.org, 2008
- Singleton T., **Auditing the IT Auditors**, ISACA Journal, Vol. 3, 2013