فصلنامه پژوهش های معاصر در علوم مدیریت و حسابداری
سال سوم، شماره ۱۰، پاییز ۱۴۰۰
ISSN: ۲۶۷۶-۶۳۱۰
www. jocrimas.ir

حسابرسی فناوری اطلاعات

نیلوفر ذلک زاده [۱]

[۱] حسابرس ارشد دیوان محاسبات استان چهارمحال و بختیاری- کارشناس ارشد مدیریت بازرگانی

چکیده

با ورود فناوری‌های اطلاعات به عرصه‌ی تجارت، تغییرات عظیمی در محیط تجاری رخ داده است. اقتصاد جهانی بیشتر از هر زمان دیگر به همدیگر وابسته شده اند و زیرساخت های الکترونیکی و تجارت در فرآیندهای کسب و کار در سراسر جهان یکپارچه شده است و نیاز به کنترل و حسابرسی فناوری اطلاعات بیش از پیش افزایش یافته است. از این رو حسابرسان باید خود را با این محیط جدید و پیچیده انطباق دهند. در این محیط پیچیده استفاده از روش حسابرسی کامپیوتری و حسابرسی IT ضرورت بیشتری خواهد یافت. توسعه‌ی فناوری اطلاعات، در عین حال که محیط حسابرسی را پیچیده‌تر می‌سازد، زمان، شیوه‌ها و ابزارهای جدیدتری را نیز برای مواجهه شدن حسابرسان با کار حسابرسی فراهم می‌کند. با استفاده از روشهای حسابرسی مبتنی بر رایانه، تجزیه وتحلیل حجم انبوهی از داده ها در مدت زمان کوتاهی ممکن شده و خطاها، تقلبها و سوء استفاده ها با سهولت بیشتری کشف می شوند.

واژه‌های کلیدی: حسابرسی، فناوری اطلاعات، حسابرسی فناوری اطلاعات

مقدمه

مفهوم حسابرسی فناوری اطلاعات (IT) نخستین بار در اواسط دهه‌ی ۱۹۶۰ میلادی مطرح شد. حسابرسی IT سیستمی مبتنی بر فناوری اطلاعات با هدف کمک به حسابرسان در فرایند برنامه‌ریزی، اجرا، کنترل، تکمیل و هدایت عملیات حسابرسی است. حسابرسی IT را حسابرسی پردازش اتوماتیک داده‌ها (ADP) و حسابرسی کامپیوتری نیز می‌نامند. این نوع از حسابرسی قبلا با عنوان حسابرسی پردازش الکترونیکی داده‌ها (EDP) نیز نامیده می‌شده است.

حسابرسی فن‌آوری اطلاعات، حسابرسان را قادر می‌سازد تا به طور مستقیم و از طریق ابزارهای ارتباطی پیشرفته به موضوعات حسابرسی دسترسی داشته باشند. امروزه که در بسیاری از شرکت‌ها از سیستم‌های مختلف پردازش الکترونیکی داده‌ها (EDP) برای پردازش اطلاعات حسابداری استفاده می‌کنند، تنها راه بررسی و اعتباردهی به گزارش‌ها، حسابرسی IT است.

در واقع حسابرسان مستقل که نقش اصلی شان اعتباردهی به اطلاعات حسابداری است، برای ارائه‌ی خدمات حسابرسی گسترده‌تر و به‌روز در خصوص داده‌های الکترونیکی حسابداری و نیز برای جمع‌آوری و آزمون اطلاعات حسابداری و افزایش کارایی در حسابرسی به حسابرسی فناوری اطلاعات رو آورده‌اند.

- ✓ حسابرسی IT فرایند سیستماتیک جمع آوری و ارزیابی بی‌طرفانه‌ی شواهد پشتوانه‌ی یک یا چند ادعا از سیستم‌های اطلاعاتی، شیوه‌ها و عملیات یک سازمان است. ارزیابی شواهد کسب شده در این حسابرسی نشان می‌دهد که اگر سیستم‌های اطلاعاتی ایمن باشد؛ داده‌های نگهداری شده صحیح و عملیات شرکت به طور کارا و موثر اهداف سازمانی را تحقق می‌بخشد. این نوع از حسابرسی ممکن است همزمان با حسابرسی صورت‌های مالی، حسابرسی داخلی و یا دیگر اشکال خدمات اعتبار بخشی انجام شود.
- ✓ حسابرسی فناوری اطلاعات (IT) یا حسابرسی سیستم‌های اطلاعاتی، آزمون کنترل‌های یک ساختار فناوری اطلاعات است.

در بررسی رابطه حسابرسی و کامپیوتر دو جنبه را می توان متصور بود :

الف- تاثیر کامپیوتر بر محیط واحد تجاری که حسابرس باید آن را بررسی و حسابرسی نماید(حسابرسی فناوری اطلاعات).

ب- استفاده از کامپیوتر برای انجام حسابرسی .

مهمترین عواملی که منجر به لزوم انجام حسابرسی فناوری اطلاعات شدند :

- حسابرسان متوجه تواناییهای نهفته در سیستم های کامپیوتری برای انجام عملکرد گواهی دادن شدند.
- شرکتها پردازش و مدیریت اطلاعات را در سازمان خود به رسمیت شناختند بطوری که رایانه ها منابع کلیدی برای رقابت در محیط کسب و کار، مشابه سایر منابع با ارزش کسب و کار در سازمان شدند و در نتیجه ، نیاز به کنترل و حسابرسی آنها حیاتی گردید.
- انجمن های حرفه ای و سازمان ها و نهادهای نظارتی دولتی نیاز به کنترل و حسابرسی فناوری اطلاعات را به رسمیت شناختند.

تأثیر فناوری اطلاعات بر فرآیند حسابرسی

- سیستم های اطلاعاتی حسابداری و مکانیزم های پردازش الکترونیکی داده های اقتصادی و تجاری،کارکرد حرفه حسابرسی را به شدت تحت تأثیر قرار داده است. پردازش و گزارش اطلاعات حسابداری توسط حسابداران و اعتباردهی به آن از سوی حسابرسان در محیط سیستم های اطلاعاتی حسابداری، مباحث و گزینش های جدیدی را در برابر حرفه حسابرسی قرار داده است که مستلزم واکنش متقابل از طرف حرفه حسابرسی است. بر این اساس حرفه حسابرسی ناگزیر است خود را با تحولات فناوری اطلاعات همگام سازد تا ضمن حفظ جایگاه حرفه ای خود در جامعه به عنوان مرجع اعتباردهی اطلاعات مالی شرکت ها، از فرصت های جدیدی که فناوری اطلاعات عرضه می نماید نیز به طور مطلوب بهره جوید.
- یک حسابرس باید در کسب و کار از مشتری برتر باشد. به همین منوال یک حسابرس سیستم اطلاعاتی باید از یک مدیر سیستم اطلاعاتی درون تشکیلات، با سیستم آشناتر باشد. در دنیای در حال تغییر فناوری اطلاعات، اگر چه رسیدن به چنین درجه بالایی از مهارت رویایی ولی یک وظیفه است. هدف فناوری اطلاعات تغییر اهداف حسابرسی نیست، بلکه ممکن است ماهیت (طبیعت)، میزان (دامنه) و زمانبندی فرایندحسابرسی را تحت تأثیر قرار دهد.
- پردازش الکترونیکی داده ها از دو جنبه بر حسابرسی صورت های مالی تأثیر دارد. یک جنبه، اثر آن در مطالعه و ارزیابی کنترل های داخلی است که شامل ارزیابی کنترل های عمومی مرکز خدمات رایانه ای و کنترل های کاربردی نرم افزارهای مالی است. جنبه دیگر، اثر پردازش الکترونیکی داده ها بر حسابرسی در مرحله آزمون محتوای صورت های مالی است. هدف حسابرسی در مرحله تأمین شواهد کافی به منظور ارایه نظر درباره صورت های مالی است. نگرانی حسابرسان درباره فرآیند توزیع داده ها است. همچنین، حسابرسان درباره صحت و کامل بودن دادهها موقعی که داده ها بین کامپیوتر مرکزی (سرور) و شخصی (مشتری) منتقل میشوند، نگران هستند.

ریسک ذاتی خاص فناوری اطلاعات

فناوری اطلاعات، عوامل ریسک خاصی را برای حسابداری، حسابرسی و سامانه ها به همراه دارد؛ به این معنی که خود فناوری اطلاعات در ارتباط با سامانه ها، فرایندهای کسب و کار تجاری و پردازش مالی و حسابداری، برای واحد تجاری ریسک به همراه می آورد. این ریسک، مختص فناوری اطلاعات است؛ به این معنی که بدون وجود فناوری اطلاعات دستکم در این سطح، این ریسک نیز به وجود نمی آید. برای این کار، نیاز است تا فردی حرفه ای همچون حسابرس فناوری اطلاعات، ریسک ذاتی مرتبط با فناوری اطلاعات را شناسایی و ارزیابی کند. عوامل ریسک پیشگفته دربرگیرنده موضوع های مرتبط با سامانه ها مانند ایجاد سامانه ها، مدیریت تغییرات، آسیب پذیری ها و دیگر عوامل خاص فناوری است. بدون به کار گماردن متخصصان حرفه ای فناوری اطلاعات، چنین ریسکی ممکن است از نظر دور بماند و موجب ایجاد ضرر برای واحد تجاری شود. برای نمونه، دانشگاهی تجربه ای را در ارتباط با سامانه های اعطای کمک مالی، از سر گذرانده است (میلیونها دلار کمک مالی به اشتباه اعطا شد).

با این فرض که تقریباً تمام واحدهای تجاری، فناوری اطلاعات را در سطوح مختلفی به کار می گیرند، زمان آن فرا رسیده است که آنها برای ارزیابی ریسک ذاتی فناوری اطلاعات خود، از خدمات حسابرسان فناوری اطلاعات بهره مند شوند. حسابرسان فناوری اطلاعات به طور ویژه برای انجام این وظیفه آموزش دیده و از مهارت برخوردار هستند. حسابرسان فناوری اطلاعات توانایی شناسایی ماهیت و ریسک فناوریهای اطلاعات و سامانه ها را دارند.

کارهایی که در حسابرسی IT باید انجام شود را می‌توان با سوالات زیر خلاصه کرد:

- ✓ آیا در صورت نیاز سازمان، سیستم‌های کامپیوتری همیشه برای شرکت قابلیت استفاده را خواهد داشت؟(در دسترس بودن)
- ✓ آیا اطلاعات موجود در سیستم‌ها تنها برای کاربران مجاز افشا خواهند شد؟(محرمانه بودن)
- ✓ آیا اطلاعات تهیه شده برای سیستم‌ها همواره صحیح، قابل اتکا و به‌هنگام است؟(درستی)

حسابرسی IT بر ریسک‌های تعیین‌کننده ی مربوط به دارایی‌های اطلاعاتی تمرکز کرده، تا با ارزیابی صحیح کنترل‌ها، این ریسک را کاهش دهند. با اجرای کنترل‌های مربوطه، اثر این ریسک‌ها را می‌توان به حداقل رساند، اما نمی‌توان همه این ریسک‌ها را به طور کامل از بین برد.

اجزای اولیه حسابرسی فناوری اطلاعات :

- اول، استفاده از روش های حسابرسی سنتی، روش های کنترل داخلی و کنکاش و تحلیل برروی فلسفه کنترل
- دوم، مدیریت سیستم های اطلاعاتی می باشد، که روش های لازم برای رسیدن به طراحی و اجرای موفقیت آمیز سیستم ها را فراهم می کند.
- سوم ، زمینه علوم کامپیوتر و دانش لازم در مورد مفاهیم کنترل ، نظم و انضباط ، نظریه ها، مدل های رسمی که زمینه ی طراحی سخت افزار و نرم افزار ها را به عنوان پایه ای برای حفظ اعتبار داده ها ، قابلیت اطمینان، و صداقت فراهم می کند.

بدین ترتیب حسابرسی فناوری اطلاعات بخشی جدایی ناپذیر از تابع حسابرسی است، زیرا پشتیبانی از قضاوت حسابرس در کیفیت پردازش اطلاعات توسط سیستم های کامپیوتری را بر عهده دارد. بطوریکه در ابتدا، به عقیده حسابرسان، مهارتهای حسابرسی فناوری اطلاعات به عنوان منابع تکنولوژیکی برای کارکنان حسابرسی به شمار می آمد. کارکنان حسابرسی اغلب به این منابع به عنوان کمک های فنی نگاه میکرند.

بسیاری از شرکتها از سیستمهای مختلف پردازش الکترونیکی داده ها برای پردازش اطلاعات حسابداری استفاده می کنند، تنها راه بررسی و اعتباردهی به گزارشها، حسابرسی فناوری اطلاعات است. از این رو، حسابرسان مستقل که نقش اصلیشان اعتباردهی به اطلاعات حسابداری است، برای ارائه خدمات حسابرسی گسترده تر و به روز در خصوص داده های الکترونیکی حسابداری و نیز برای جمع آوری و آزمون اطلاعات حسابداری و افزایش کارایی در حسابرسی به حسابرسی فناوری اطلاعات روی آورده اند.

آیا حسابرسان صورتهای مالی باید از دانش و مهارتهای حسابرسان فناوری اطلاعات برخوردار باشند؟

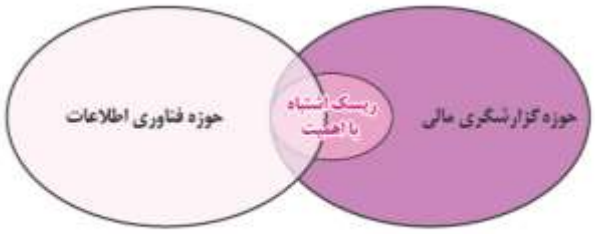
حسابرسان صورتهای مالی یا باید خود از دانش و مهارتهای لازم برای حسابرسی حوزه هایی از فناوری اطلاعات که مرتبط و مربوط گزارشگری مالی است برخوردار باشند و یا از خدمات حسابرسان فناوری اطلاعات در این زمینه استفاده کنند. در همین راستا بیشتر مؤسسه‌های حسابرسی بزرگ و به‌نام در سطح بین‌الملل، از واحد حسابرسی فناوری اطلاعات در ترکیب سازمانی خود برخوردارند. برای تعیین میزان مشارکت حسابرسان فناوری اطلاعات در حسابرسی صورتهای مالی، به‌نحوی که نه خیلی کم و نه خیلی زیاد باشد، ضوابط حسابرسی مبتنی بر ریسک باید مدنظر قرار گیرد.

برای این منظور ابتدا باید دامنه گزارشگری مالی مشخص شود (طبق شکل) و با در نظر داشتن محدوده یادشده به پرسشهای زیر پاسخ داده شود:

• چه سیستمها و روشهایی اعم از دستی و خودکار برای گزارشگری مالی استفاده می شود؟

•اطلاعات کدام حسابها و گروههای معاملات و موارد افشا در گزارشگری مالی دخیل هستند؟

•در چرخه فرایند گزارشگری مالی چه پردازشهایی اعم از دستی و خودکار به وقوع می پیوندد؟



ارتباط حسابرسی فناوری اطلاعات و حسابرسی صورتهای مالی

سپس لازم است حوزه فناوری اطلاعات شناسایی شود تا اجزایی از این حوزه که مربوط و مرتبط به حوزه گزارشگری مالی است تعیین شود. از این طریق، دامنه کار حسابرسی فناوری اطلاعات محدود به شناخت و احتمالاً ارزیابی کنترلهای حاکم بر این اجزا خواهد شد همانطور که در شکل مشخص است، تنها بخشی از حوزه فناوری اطلاعات به فرایند گزارشگری مالی مربوط است و کنترلهای آن به عنوان کنترلهای مرتبط با حسابرسی صورتهای مالی (طبق تعریف استاندارد ۳۱۵ حسابرسی) در نظر گرفته می شود، پس این بخش باید مورد شناخت و در صورت ضرورت مورد ارزیابی حسابرس قرار گیرد. اجزای این بخش در عمل می تواند شامل روشهای گردآوری ،پردازش، ذخیره سازی و انتقال داده ها باشد.

طبق استاندارد حسابرسی شماره ۳۱۵، فرایند کسب شناخت باید به نحوی انجام شود که حسابرس را قادر به تشخیص و براورد خطرهای تحریف با اهمیت که متشکل از خطر ذاتی و خطر کنترل است نماید. در محیطهای بهره مند از فناوری اطلاعات، خطر کنترل وابستگی زیادی به فناوری اطلاعات دارد؛ از اینرو تعیین ریسکهای ناشی از کنترلهای فناوری اطلاعات و از میان آنها شناسایی ریسکهایی که ممکن است اشتباههای بااهمیت در صورتهای مالی ایجاد کنند، امری اجتناب ناپذیر است.

در اینجا توجه به این نکته ضروریست که وسعت حوزه فناوری اطلاعات الزاماً تابع اندازه سازمانها نیست بلکه تابع سطح کمال فناوری اطلاعـات (Level of IT Sophistication) در هر سازمان است. یک سازمان کوچک ۵۰ نفری که برای توزیع محصولات یا خدمات، برای اعلام داده های حقوق کارکنان به بانک و برای دسترسی آنلاین مدیران به اطلاعات گردش عملیات برای اداره امور شرکت از فناوری اطلاعات استفاده می کند، در نهایت متکی به کنترلهای فناوری اطلاعات در فرایندهای گزارشگری مالی است، در سطحی متوسط به بالا از کمال فناوری اطلاعات طبقه بندی می شود .در نقطه مقابل، کارخانه ای با انبارهای متعدد و هزاران مشتری و صدها کارگر، ولی متکی به نرم افزارهای تجاری گوناگون که برای تهیه گزارشهای مالی به یک سرور متصل شده اند، درسطحی پایین از کمال فناوری اطلاعات قرار دارد . هرچه سطح کمال فناوری اطلاعات در سازمان پایینتر باشد، حوزه فناوری اطلاعات در آن سازمان کوچکتر و دامنه کار حسابرسی فناوری اطلاعات برای حسابرسان صورتهای مالی محدودتر خواهد بود و بالعکس.

مستندات حسابرسی در حسابرسی IT

هیئت استانداردهای انجمن حسابرسان سیستم‌های اطلاعاتی رایانه‌ای، مستندات حسابرسی را این‌گونه تعریف می‌کند:

مدارک انجام شدن کار حسابرسی و شواهد پشتوانه یافته‌های حسابرسی و نتیجه‌گیری‌های حسابرس از سیستم‌های کامپیوتری.

در واقع هر چیزی که در ارتباط با موضوع مورد رسیدگی، دیده، شنیده، مشاهده و آزمون می‌شود، شواهد حسابرسی است و باید مستند گردد. از سوی دیگر در محیط تجاری امروزی، شرکت‌ها باید اطلاعاتی به‌روز و قابل اتکا برای ذینفعان فراهم کنند. امروزه بسیاری از شرکت‌های پیشرفته رویدادهای مالی خود را بدون مستندات کاغذی و به صورت الکترونیکی‌شناسایی، ثبت، اندازه گیری و گزارش می‌کنند. بدون تردید حسابرسی در چنین محیطی با حسابرسی سنتی که همواره با مستندات کاغذی همراه بوده، تفاوت‌های زیادی دارد.

امروزه در بسیاری از کشورهای جهان استفاده از مبادلات الکترونیکی داده‌ها (EDI) کاملاً مرسوم شده است استفاده از مبادلات الکترونیکی باعث می‌شود تا شرکت‌ها با انجام فعالیت‌های تجاری بدون استفاده از مستندات کاغذی به طور غیر مستقیم در زمان و پول صرفه‌جویی کنند. اما در این راستا تحول اساسی که می‌تواند در حرفه‌ی حسابرسی رخ دهد، این است که سرمایه گذاران با دسترسی به اطلاعات به‌روز بانک‌های اطلاعاتی شرکت‌ها، ممکن است دیگر علاقه‌ی چندانی به صورت‌های مالی سالانه مبتنی بر اطلاعات تاریخی و در نتیجه اظهار نظر ادواری حسابرسان در این مورد، نداشته باشند. در مقابل، تقاضای ذی‌نفعان از حرفه‌ی حسابرسی تغییر کرده و خواهان این هستند که بدانند حسابرسان در مورد کیفیت و قابلیت اتکای اطلاعات به‌روز موجود در بانک‌های اطلاعاتی شرکت‌ها چه اظهار نظری می‌کنند. در واقع آیا تمام این‌اطلاعات مندرج در بانک‌های اطلاعاتی مورد حسابرسی قرار گرفته و قابل اتکا است؟

کنترلهای فناوری

بیانیه استانداردهای حسابرسی شماره ۷۸ با عنوان بررسی ساختار کنترل داخلی در حسابرسی صورتهای مالی بیان میکند: کنترل داخلی فرایندی است برای فراهم کردن اطمینان معقول از دستیابی به هدفهای الف) اعتمادپذیری گزارشگری مالی، ب) اثربخشی و کارایی عملیات، و ج) رعایت قوانین و مقررات مربوط.

حسابرسان برای دستیابی به درک مورد نیاز از کنترلها باید آشنایی فزاینده ای با کنترلهای فناوری اطلاعات بیابند؛ ولی عمده حسابرسان آگاهی کافی از این موضوع ندارند. هیئت تدوین استاندارد حسابرسی این مشکل را تشخیص داده و در بیانیه استاندارد حسابرسی شماره ۷۸، رهنمودهای بیشتری درباره کنترلهای فناوری اطلاعات ارائه کرده است. متاسفانه این بیانیه تاثیر اندکی بر نحوه اجرای حسابرسی به وسیله مؤسسه های حسابرسی داشت.

بنابراین هیئت تدوین استانداردهای حسابرسی در بیانیه شماره ۹۴ تاثیر فناوری اطلاعات بر بررسی کنترلهای داخلی به وسیله حسابرسان را مورد توجه قرار داد. به صورت مختصر، در این استاندارد چنین بیان شده است: «بشتابید حسابرسان؛ دیگر نمی توانید فناوری را نادیده بگیرید!». برای خنثی نمودن تغییرهای فناوری برای مقابله با چالش سریع در حسابرسیِ صاحبکار با ریسک بالا یا پیچیده ، مؤسسه های حسابرسی باید استفاده از متخصصان فناوری را به عنوان عضوی از گروه، مدنظر قرار دهند.

به طور مسلم این همکاری منجر به حسابرسی با کیفیت بالاتری خواهد شد و احتمال دارد گروه حسابرسی با شناسایی ضعفها و فرصتهای فناوری اطلاعات، خدمات بهتری را به صاحبکاران ارائه نماید.

برای درک بهتر کنترلهایی که ممکن است در شرکت وجود داشته باشد، از الگوی مفهومی موسسه آدیت واچ (Audit Watch) استفاده شده است در این الگوی مفهومی، مسیر حرکت یک معامله از آغاز تا مقصد نهایی که همانا صورتهای مالی است، به صورت "جریان" نمایش داده شده است:

کنترلهای ورودی: موجب اطمینان از ورود صحیح اطلاعات به سیستم رایانه ای می شوند. برای مثال، حسابداری قبل از وارد کردن اطلاعات به رایانه اثبات می کند که همه سفارشهای خرید به نحو مناسبی تایید و کدگذاری شده است. طی سالها، حسابرسان به هنگام کسب شناخت از سیستم صاحبکار روی این نوع کنترلها تمرکز کرده اند.

کنترلهای فناوری اطلاعات: کنترلهایی خودکارند که به پیشگیری از تحریفها کمک میکنند. با وجود رواج فزاینده فناوری اطلاعات در دنیای تجارت، بسیاری از حسابرسان این کنترلها را نمی فهمند و در نتیجه از آنها دوری میکنند .

کنترلهای خروجی: پس از پردازش اطلاعات در سیستم رایانه ای وارد عمل می شوند. این کنترلها در هنگام بررسی ستانده های تولیدشده به وسیله سیستم، مورد استفاده قرار می گیرد. برای مثال اگر برای اطمینان از ثبت کلیه بدهی ها، پرداخته ای بعد از تاریخ ترازنامه کنترل شود، این کنترلها می توانند بسیار مفید باشد. به همین دلیل، تعداد فزاینده ای از حسابرسان برای درک بهتر نحوه عملکرد آنها زمان صرف می کنند .

کنترل‌های حسابرسی IT

بسیاری از صاحب نظران تلاش می‌کنند تا کنترل‌های حسابرسی را به حوزه‌های متعددی تقسیم بندی کنند. برخی کارشناسان حسابرسی ITدر حوزه‌ی بیمه‌ی اطلاعات، بیان می‌کنند که صرف‌نظر از نوع حسابرسی اجرا شده، سه نوع کنترل اصلی در حیطه‌ی حسابرسی IT وجود دارد؛ کنترل‌های امنیتی، کنترل‌های دسترسی و کنترل‌های اطلاعات حسابداری.

در سطح اساسی‌تر می‌توان نشان داد که این کنترل‌ها هر کدام شامل سه سطح از کنترل‌های پایه‌ای‌تر است: کنترل‌های پیشگیری کننده-حفاظتی، کنترل‌های کشف‌کننده و کنترل‌های اصلاح کننده-واکنشی.

در سطح اول، کنترل‌های پیشگیری کننده -حفاظتی حوزه‌ی گسترده‌ای داشته و تاکید آن بر انطباق رفتارها با قوانین پذیرفته شده می‌باشد. به عنوان مثال، یک مجموعه از قوانین حسابداری عمومی تعریف شده است که باید به طور عمومی همه‌ی شرکت‌های بازرگانی آن را رعایت کنند. هر بخشی از شرکت باید به طور کلی پاسخ‌گوی تطابق روش‌های مالی و حسابداری جاری به‌کارگرفته شده با قوانین پذیرفته‌شده باشد. استانداردهای حسابداری و الزامات بورس را می‌توان به عنوان کنترل‌های پیشگیری‌کننده یا حفاظتی نام برد.

در سطح دوم، کنترل‌های کشف‌کننده‌هستند که اغلب به عنوان "کنترل‌های حسابرسی" تلقی می‌شوند که البته لزومی ندارد آنها را صرفاً به کنترل‌های حسابرسی محدود کنیم. هر عاملی که فعالیتی نظارتی را اجرا می‌کند، می‌تواند به عنوان یک کنترل کشف‌کننده تلقی شود. در واقع یکی از کنترل‌هایی که شرکت‌ها باید علاوه بر کنترل‌های حفاظتی انجام

دهند، این است که باید نتایج مالی خود را به وسیله‌ی یک حسابدار رسمی مستقل مورد حسابرسی قرار دهد. در حقیقت هر حسابرس به عنوان یک کنترل کشف‌کننده عمل می‌کند. اگر سازمان مورد رسیدگی به طور عمومی از قوانین مربوطه‌ی حسابداری پیروی کرده باشد، حسابرس باید بتواند ایرادات جزئی را که موجب می‌شود برخی از کنترل‌های شرکت به طور کارا و موثر عمل نکند شناسایی کند.

سطح سوم کنترل‌های حسابرسی IT، شامل کنترل‌های اصلاح‌کننده- واکنشی است. این کنترل‌ها در پاسخ به کنترل کشف‌کننده واکنش نشان می‌دهند. پاسخ‌دهی از چنین طریقی در واقع نقش آگاهی‌بخش و تصحیح‌کننده را ایفا می‌کند. کمیته‌ی حسابرسی یک شرکت مورد بررسی و یا خود مقام ناظر بورس می‌توانند بر مبنای گزارش‌های ایجاد شده به وسیله‌ی حسابرسان مستقل، برخی از اعمال اصلاح‌کننده را انجام دهند. از این رو می‌توان آن‌ها را به عنوان کنترل‌های اصلاح کننده یا واکنشی به حساب آورد.

حال ممکن است این سوال مطرح شود که وقتی سازمان‌های تحت حسابرسی IT، با مشکلاتی مثل تحمل برخی زیان‌ها یا خطر کشف رمزهای اینترنتی و سایر مسایل امنیتی در در محیط فناوری اطلاعات قرار می‌گیرند، شرکت‌هایی که فاقد کنترل‌های مناسب برای این محیط هستند، باید از چه کنترل‌هایی استفاده کنند؟ در حقیقت نمی‌توان راهکاری عام برای پاسخ به این سوال داد، اما می‌توان به طورکلی گفت که آن‌ها الزاما باید از هر سه سطح کنترل‌های مربوط به حسابرسی IT (پیشگیری‌کننده، کشف‌کننده و واکنشی) استفاده کنند.

کنترلهای فناوری اطلاعات و الزامات استانداردهای حسابرسی

در استانداردهای حسابرسی ۳۱۵ و ۳۳۰ بیان شده: حسابرس هنگام شناخت از کنترلهای مرتبط با حسابرسی باید اجرای روشهایی افزون بر پرس و جو از کارکنان واحد تجاری، طراحی آن کنترلها را ارزیابی کند و مشخص کند که آیا کنترلها اعمال شده اند یا خیر.

استفاده از فناوری اطلاعات نحوه اعمال فعالیتهای کنترلی را تحت تاثیر قرار می دهد. حسابرس باید از روشهای موجود در سیستمهای فناوری اطلاعات که به وسیله آنها معاملات شروع، ثبت، پردازش، در صورت لزوم اصلاح، به حسابهای کل منتقل و در صورتهای مالی گزارش می شود، شناخت کسب کند. حسابرس هنگام شناخت فعالیتهای کنترلی واحد تجاری، باید از نحوه برخورد واحد تجاری با خطرهای ناشی از فناوری اطلاعات، شناخت کسب کند.

هنگامی که واحد تجاری فعالیتهای خود را با استفاده از فناوری اطلاعات انجام می دهد و هیچگونه مستنداتی درباره معاملات به جز آنچه به وسیله سیستم فناوری اطلاعات ایجاد می شود وجود نداشته باشد، حسابرس ملزم است آزمون کنترلها، به خصوص کنترلهای فناوری اطلاعات را اجرا کند.

از نظر حسابرس، کنترلهای حاکم بر سیستمهای اطلاعاتی هنگامی مؤثر است که درستی اطلاعات و امنیت داده های مورد پردازش در این سیستمها را حفظ کند و شامل کنترلهای اثر بخش "عمومی" و "کاربردی" فناوری اطلاعات باشد.

در استاندارد حسابرسی ۳۱۵ این کنترلها به شرح زیر تشریح شده است:

کنترلهای عمومی فناوری اطلاعات: سیاستها و روشهایی است که به نرم افزارهای کاربردی متعددی مربوط می شود و از کارکرد مؤثر کنترلهای کاربردی پشتیبانی میکند، درستی اطلاعات و امنیت داده ها را حفظ می کنند به طور معمول شامل کنترلهای مربوط به "مرکز داده ها و عملیات شبکه"، "تحصیل، تغییر و نگهداری نرم افزار سیستم"، "تغییر برنامه"،"امنیت دسترسی" و "تحصیل، توسعه و نگهداری سیستم کاربردی" است. این کنترلها به طور معمول به منظور برخورد با خطرهای ناشی از مواردی چون موارد زیر طراحی و اجرا می شوند :

دسترسی غیرمجاز به داده ها، که ممکن است موجب از بین رفتن داده ها یا تغییر نابه جا در داده ها، شامل ثبت معاملات غیر مجاز یا واهی، یا ثبت نادرست معاملات شود،

احتمال برخورداری کارکنان فناوری اطلاعات از امکان دسترسی بیش از حد نیاز برای انجام وظایف خود و از این رو، نقض تفکیک وظایف،

تغییرات غیر مجاز داده ها در پرونده های اصلی،

تغییرات غیر مجاز در سیستمها یا برنامه ها،

کوتاهی در انجام تغییرات لازم در سیستمها و برنامه ها،

دخالتهای دستی نامناسب، و

احتمال از دست رفتن داده ها یا ناتوانی در دسترسی به داده های مورد نیاز.

کنترلهای کاربردی فناوری اطلاعات: روشهای دستی یا خودکاری است که به طور معمول در سطح فرایندهای تجاری اجرا می شود و برای پردازش معاملات به وسیله نرم افزارهای کاربردی به کار می رود. کنترلهای کاربردی می تواند ماهیت پیشگیری کنندگی یا کشف کنندگی داشته باشد و برای به دست آوردن اطمینان از درستی سوابق حسابداری طراحی می شود. از این‌رو، کنترلهای کاربردی به روشهای مورد استفاده در انجام، ثبت، پردازش و گزارش معاملات یا دیگر اطلاعات مالی مربوط می شود.

این کنترلها برای اطمینان از موارد زیر هستند:

- داده وارده به سیستم، دقیق، کامل، مجاز و اصلاح شده است،
- داده در مدت زمان قابل قبول تحت پردازشهای مد نظر قرار می گیرد،
- داده ذخیره شده، صحیح و کامل است،
- خروجیها صحیح و کامل هستند، و
- سابقه قابل ردیابی جریان داده از هنگام ورود تا ذخیره سازی و خروج احتمالی (حذف داده)، در قالب یک رکورد اطلاعاتی وجود دارد.

انواع مختلف کنترلهای کاربردی برای دستیابی به هدفهای یاد شده عبارتند از:

- کنترلهای ورودی
- کنترلهای پردازشی
- کنترلهای خروجی
- کنترلهای یکپارچگی

- پی جویی مدیریت

چگونگی اجرای یک راهبرد حسابرسی فناوری اطلاعات اثربخش برای هر سازمان

استقلال: پیش‌نیاز حسابرسی فناوری اطلاعات اثربخش، این است که کوشش برای انجام حسابرسی به‌گونه‌ای پایه‌ریزی شود که حسابرس در عمل و در ظاهر از واحد مورد رسیدگی مستقل باشد. جایگاه حسابرس فناوری اطلاعات از نظر تشکیلاتی، نبایستی زیر مجموعه واحد فناوری اطلاعات سازمان باشد. انجام این کار با جذب حسابرسان سیستمهای اطلاعاتی دارای صلاحیت حرفه‌ای آغاز می‌شود. خدمات حسابرسی فناوری اطلاعات ممکن است از سوی کارکنان واحد حسابرسی داخلی یا مشاوران و شرکتهای برون‌سازمانی فراهم شود.

تخصص: در حوزه تخصصی حسابرسی فناوری اطلاعات، هیچ سابقه کاری مقتضی این نوع حسابرسی وجود ندارد. برخی از حسابرسان فناوری اطلاعات با عنوان حسابرسان مالی یا عملیاتی این کار را آغاز می‌کنند، در حالی که دیگران از سایر تخصصهای فناوری اطلاعات، به حسابرسی فناوری اطلاعات می‌آیند. در هر حال، انجمن حسابرسی و کنترل سیستمهای اطلاعاتی(ISACA)[۱] به حسابرسان فناوری اطلاعات، یک گواهی معتبر جهانی تحت عنوان گواهینامه حسابرس سیستمهای اطلاعاتی(CISA)[۲] اعطا می‌کند. افراد حرفه‌ای با دریافت این عنوان در واقع نشان می‌دهند که مهارت لازم برای انجام کاری که از آنان انتظار می‌رود را با پشت سر گذاشتن یک آزمون سخت و کسب تجربه، آموزش و صلاحیتهای شخصیتی به‌دست آورده‌اند. همچنین از آنان انتظار می‌رود که از استانداردها و رهنمودهای حرفه‌ای پیروی نمایند. در حال حاضر به حسابرسان دارای گواهینامه سیستمهای اطلاعاتی نیازی مبرم است، چون سازمانها کوشش می‌کنند که در برابر الزامات قانون ساربینز-اکسلی و دیگر موارد ابتکار عمل و قانونگذاری جدید در سطح جهانی پاسخگو باشند.

برنامه حسابرسی : کار حسابرسی فناوری اطلاعات برای سازمان بایستی براساس برنامه حسابرسی مبتنی بر ریسک انتخاب شود. حسابرسیها باید به‌طور مستقیم به‌سوی حوزه‌هایی هدایت شوند که سازمان بیشترین منافع را از آنها دریافت خواهد کرد. فرد تهیه‌کننده برنامه باید عناصر ریسک را به گونه‌ای تعیین کند که برای سازمان مناسب است.

عناصر ریسک اثربخش در برگیرنده موارد زیر است:

- اهمیت سیستم برای سازمان،
- فاصله زمانی با حسابرسی پیشین،
- حجم داراییهای موجود، و
- جدید بودن سیستم.

[۱] Information Systems Audit and Control Association (ISACA)

[۲] Certified Information Systems Auditor (CISA)

گرداوری اطلاعات: هر حسابرسی بایستی بر شناخت کلی از حوزه مورد رسیدگی متکی و دربرگیرنده اطلاعاتی مانند موارد زیر باشد:

• الزامات تجاری،
• ریسکها،
• نقشها و مسئولیتها،
• سیاستها و رویه‌ها،
• رعایت قوانین و مقررات، و
• کنترلهای داخلی موجود.

حسابرسان می‌توانند این شناخت را از طریق مصاحبه با افراد کلیدی و بررسی اسناد سازمان به‌دست آورند.

تعیین هدفهای کنترل: هدف کنترل فناوری اطلاعات عبارت است از "ارائه یک بیانیه از نتیجه یا هدفی مورد انتظار که با اجرای رویه‌های کنترل در یک فعالیت فناوری خاص به‌دست می‌آید." به عبارت دیگر، کنترلی است که حسابرس و مدیر تمایل دارند آن را به‌کارگیرند تا اطمینان یابند یک جنبه از فعالیت فناوری اطلاعات به‌درستی کنترل می‌شود انجمن راهبری فناوری اطلاعات چارچوبی بین‌المللی به نام هدفهای کنترل اطلاعات و فناوری مرتبط را فهرست می‌کند که پوشش دهنده کل دامنه حسابرسی فناوری اطلاعات هم در سطح بالا و هم تفصیلی است. هدفهای کنترل اطلاعات و فناوری مرتبط، مرجعی با اطلاعات گسترده است که به حسابرسان در تعیین این که در جستجوی چه باشند و به مدیریت درباره مسئولیتهای رو به رشد برای مدیریت درست فناوری اطلاعات، کمک می‌کند. اهداف کنترل اطلاعات و فناوری مرتبط، به طور دوره‌ای برای انعکاس تغییرات در فناوری، حسابرسی فناوری اطلاعات و بهترین شیوه‌های نظارت بر فناوری اطلاعات، بهنگام می‌شود.

ده چالش فناوری برای حسابرسان

براساس نظرسنجی که از سوی انجمن کنترل و حسابرسی سامانه های اطلاعاتی (ISACA)- انجمن جهانی برای متخصصان خدمات اطمینان بخشیِ فناوری اطلاعات، راهبری و امنیت سایبری- انجام شده است، ده مورد از برترین چالشهایی که سازمانهای حسابرسی با آنها رو به رو هستند، عبارتند از:

۱- فناوریهای نوپدید و تغییرهای زیرساختی_ دگرگونی، نوآوری و گسیختگی،

۲- امنیت فناوری اطلاعات و حریم خصوصی- امنیت سایبری،

۳-منابع- کارکنان- چالشهای مهارتی،

۴-مدیریت زیرساخت،

۵-رایانش ابری- مجاز ی سازی،

۶-مرتبط ساختن فناوری و کسب وکار،

۷-داده های بزرگ و تحلیل داده ها،

۸-مدیریت پروژه و مدیریت تغییر،

۹-رعایت مقررات، و

۱۰-بودجه و کنترل هزینه-ها.

فناوری اطلاعات و خطر تقلب

سازمانها در همه زمینه ها نظیر انجام کسب وکار، برقراری ارتباطات و فراوری اطلاعات مالی، بر واحد فناوری اطلاعات تکیه میکنند. در شرایطی که فناوری اطلاعات به طور مناسبی طراحی نشده و یا به نحو مطلوبی کنترل نمیشود، سازمان ممکن است در معرض تقلب قرار داشته باشد. امروزه سیستمهای رایانه ای که متصل به شبکه های ملی و بین المللی هستند، در معرض تهدیدهای مداوم فضای مجازی و انواع تهدیدهایی قرار دارند که ممکن است منجر به زیانهای اطلاعاتی و مالی بیشماری شوند. فناوری اطلاعات جزو مهمی از فرایند مدیریت خطر است؛ به ویژه زمانی که خطر تقلب در دستور کار قرار گیرد. خطرهای فناوری اطلاعات شامل تهدید علیه تمامیت و پیوستگی اطلاعات و همچنین تهدیدهای نفوذکنندگان رایانه ای، امنیت سیستم و دزدی اطلاعات حساس مالی مربوط به کسب وکار سازمان است. خطر فناوری اطلاعات به هر صورتی که باشد، از قبیل نفوذ رایانه ای، جاسوسی اقتصادی، دگرگون سازی، دستبرد به اطلاعات، ویروس، دستیابی غیرمجاز به اطلاعات و سایر خطرهای تقلب فناوری اطلاعات، هر کسی را ممکن است تحت تاثیر قرار دهد. در حقیقت، فناوری می تواند از سوی افرادی که نیت ارتکاب تقلب دارند، در هریک از سه زمینه تقلبهای مربوط به شغل که به وسیله انجمن بررسی کنندگان خبره تقلب تعریف شده است، مورد استفاده قرار گیرد.

- ✓ **گزارشگری مالی متقلبانه**
- ✓ **سوء استفاده از داراییها**
- ✓ **فساد**

گزارشگری مالی متقلبانه

- **دسترسی غیرمجاز به سیستمهای عملیاتی حسابداری**- کارکنان با دسترسی غیرمجاز به دفتر کل، سیستمهای فرعی یا ابزار گزارشگری مالی، ممکن است نسبت به انجام ثبتهای متقلبانه اقدام کنند.
- **بی اثر کردن سیستمهای کنترلهای داخلی**- کنترلهای عمومی رایانه ای شامل محدودیت در دستیابی به سیستم، دستیابی محدود به سیستمهای عملیاتی و کنترلهای تعویض برنامه است. کارکنان فناوری اطلاعات ممکن است قادر به دستیابی غیرمجاز به اطلاعات محدودشده و یا تعدیل ثبتها به طور متقلبانه باشند.

سوء استفاده از داراییها

- **سرقت داراییهای مشهود**- در سازمانها، افرادی که به داراییهای مشهود (مانند پول نقد ،کالا و داراییهای ثابت) و به سیستمهای حسابداری مربوط به ثبت فعالیتهای این داراییها دسترسی دارند، میتوانند با استفاده از فناوری اطلاعات، دزدی داراییها را مخفی کنند. برای نمونه، فردی ممکن است تامین کننده ی جعلی در پرونده اصلی تامین کنندگان ایجاد کند تا پرداخت در مقابل صورتحساب جعلی خرید را تسهیل سازد؛ یا فردی کالای موجود را دزدیده و بهای اقلام سرقت شده را در حساب بهای تمام شده ثبت کند تا به این ترتیب، دارایی از ترازنامه حذف شود.

- **سرقت داراییهای نامشهود**- در دنیای امروز با توجه به اِقتصاد دانش محور و مبتنی بر خدمات، پر ارزش ترین داراییهای سازمان، داراییهای نامشهودی مانند فهرست مشتریان، تجربه های تجاری، حق اختراع و حق چاپ است . به عنوان نمونه هایی از دزدی دارایی نامشهود میتوان دزدی نرم افزارها یا محصولات، یا حق چاپ به وسیله افراد داخل یا خارج از سازمان را نام برد.

فساد

سوء استفاده از مشتریان- کارکنان داخل یا خارج از سازمان می توانند اطلاعات کارکنان یا مشریان را به دست آورند و از این اطلاعات برای دستیابی به اعتبار یا هدفهای متقلبانه دیگر استفاده کنند.

به خاطر داشته باشید که افراد متقلب در فضای مجازی، حتی مجبور به ترک خانه های خود برای ارتکاب به تقلب نیستند؛ بلکه آنها می توانند به طور عادی و از طریق شرکتهای مخابرات محلی، خدمات راه دور، ارائه دهندگان خدمات اینترنت و شبکه های ماهواره ای و بی سیم، با دیگران ارتباط برقرارکنند.

آنان می توانند قبل از حمله به سیستم های هدف در سراسر جهان و به منظور اختفای خود، به رایانه های مستقر در سایر کشورهای جهان وارد شده و از آنجا اقدام کنند. آنچه اهمیت دارد این است که تمام اطلاعات و نه تنها اطلاعات مالی از این بابت در خطر است و خسارتهای ناشی از این گونه مخاطرات روزبه روز و همزمان با تکامل فناوری، بیشتر و بیشتر می شود.

به منظور مدیریت خطر رو به رشد اداره سازمانها در عصر اطلاعات، باید زمینه های آسیب پذیری شناسایی شود و باید قادر بود مخاطرات را به روشی مقرون به صرفه کاهش داد. بنابراین، خطر فناوری اطلاعات باید در ارزیابی خطر تقلب کلی سازمان مورد توجه قرار گرفته و به طور کامل در نظر گرفته شود.

حسابرسی سیستمهای اطلاعاتی باید این اطمینان را ایجاد کند که علاوه بر حفاظت شایسته از داراییها، امکان استفاده بهینه از آنها در جهت رسیدن به هدفهای سازمانی نیز فراهم است.

منبع

-حسابرسی، فناوری اطلاعات، حسابرسی فناوری اطلاعات.