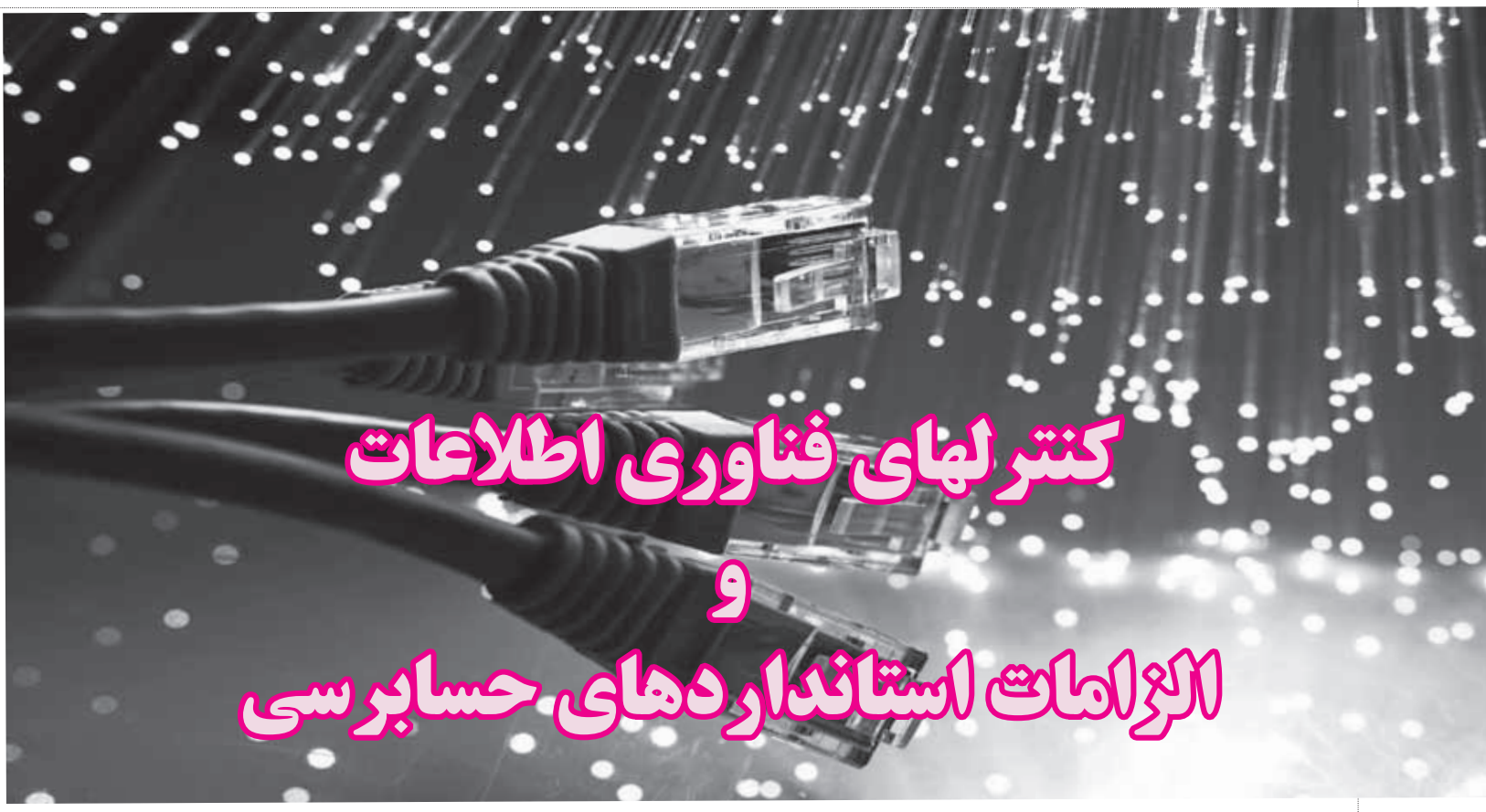


کنترلهای فناوری اطلاعات و الزامات استانداردهای حسابرسی

پرسش و دیدگاهتان را در رابطه با سلسله مطالب ستون
«حسابرسان و فناوری اطلاعات»
از طریق آدرس زیر با ما درمیان بگذارید:
hajian@hesabras.org

حسن حاجیان

سلام؛

فرارسیدن پاییز را تبریک می‌گویم. واقعاً فصل زیبایی است؛ امیدوارم فرصت پیدا کنید و از تماشای نقاشیهای طبیعت در این فصل که به قولی پادشاه فصلهاست لذت ببرید.

زرد است که لبریز حقایق شده است

تلخ است که با درد موافق شده است

شاعر نشدی وگرنه می‌فهمیدی

پاییز، بهاری است که عاشق شده است

با توجه به گسترش سیستمهای اطلاعاتی مبتنی بر فناوری اطلاعات و تأثیر درخورملاحظه آنها بر ریسک حسابرسی، در این مطلب قصد دارم نکته‌هایی را در رابطه با کنترلهای فناوری اطلاعات با شما در میان بگذارم. یکی از اصلی‌ترین دلایل پرداختن به این موضوع، ضرورت توجه به الزامات و بایدهای مندرج در استانداردهای حسابرسی در خصوص انجام حسابرسی در محیطهای وابسته به سیستمهای اطلاعاتی مبتنی بر فناوری اطلاعات است که در کشور ما شاخص‌ترین این محیطها بانکها هستند. امیدوارم این مطلب دستکم برای همپیشگان عهده‌دار حسابرسی بانکها مفید واقع شود. اجازه می‌خواهم برای شروع، مروری بر مهمترین این الزامات و بایدها در استانداردهای حسابرسی ۳۱۵ و ۳۳۰ داشته باشم.

"• حسابرس هنگام کسب شناخت از کنترلهای مرتبط با حسابرسی باید با اجرای روشهایی افزون بر پرس‌وجو از کارکنان واحد تجاری، طراحی آن کنترلها را ارزیابی کند و مشخص کند که آیا کنترلها اعمال شده‌اند یا خیر.

• استفاده از فناوری اطلاعات، نحوه اِعمال فعالیتهای کنترلی را تحت‌تأثیر قرار می‌دهد. حسابرس باید از روشهای موجود در سیستمهای فناوری اطلاعات که به‌وسیله آنها معاملات شروع، ثبت، پردازش، در صورت لزوم اصلاح، به حسابهای کل منتقل و در صورتهای مالی گزارش می‌شود، 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.

وسعت حوزه فناوری اطلاعات الزاماً تابع اندازه سازمانها نیست بلکه تابع سطح کمال فناوری اطلاعات در هر سازمان است

• از نظر حسابرس، کنترلهای حاکم بر سیستمهای اطلاعاتی هنگامی مؤثر است که درستی اطلاعات و امنیت داده‌های مورد پردازش در این سیستمها را حفظ کند و شامل کنترلهای اثربخش «عمومی» و «کاربردی» فناوری اطلاعات باشد.
• هنگامی که واحد تجاری فعالیتهای خود را با استفاده از فناوری اطلاعات انجام می‌دهد و هیچ‌گونه مستنداتی درباره معاملات به‌جز آنچه به‌وسیله سیستم فناوری اطلاعات ایجاد می‌شود وجود نداشته باشد، حسابرس ملزم است آزمون کنترلها، به‌خصوص کنترلهای فناوری اطلاعات را اجرا کند.
• هرگاه برای اجرای روشهای حسابرسی، از اطلاعات تهیه‌شده از سوی سیستمهای اطلاعاتی واحد مورد رسیدگی استفاده شود، حسابرس ملزم است درباره درستی و کامل بودن آنها شواهد حسابرسی را کسب کند."

خوشبختانه برای اطلاع از چیستی کنترلهای عمومی فناوری اطلاعات و کنترلهای کاربردی فناوری اطلاعات، زحمت زیادی لازم نیست؛ در استاندارد حسابرسی ۳۱۵ این کنترلها به‌شرح زیر تشریح شده است:

"**کنترلهای عمومی فناوری اطلاعات**، سیاستها و روشهایی است که به نرم‌افزارهای کاربردی متعددی مربوط می‌شود و از کارکرد مؤثر کنترلهای کاربردی پشتیبانی می‌کند. کنترلهای عمومی فناوری اطلاعات که درستی اطلاعات و امنیت داده‌ها را حفظ می‌کنند به‌طور معمول شامل کنترلهای مربوط به «مرکز داده‌ها و عملیات شبکه»، «تحصیل، تغییر و نگهداری نرم‌افزار سیستم»، «تغییر برنامه»، «امنیت دسترسی» و «تحصیل، توسعه و نگهداری سیستم کاربردی» است."

این کنترلها به‌طور معمول به‌منظور برخورد با خطرهای ناشی از مواردی چون موارد زیر طراحی و اجرا می‌شوند:

• اعتماد به سیستمها یا برنامه‌هایی که داده‌ها را نادرست پردازش می‌کنند، داده‌های نادرست را پردازش می‌کنند، یا هردو،
• دسترسی غیرمجاز به داده‌ها، که ممکن است موجب از بین رفتن داده‌ها یا تغییر نابه‌جا در داده‌ها، شامل ثبت معاملات غیرمجاز 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 اینرو، نقض تفکیک وظایف،
• تغییرات غیرمجاز داده‌ها در پرونده‌های اصلی،
• تغییرات غیرمجاز در سیستمها یا برنامه‌ها،
• کوتاهی در انجام تغییرات لازم در سیستمها و برنامه‌ها،
• دخالتهای دستی نامناسب، و
• احتمال از دست رفتن داده‌ها یا ناتوانی در دسترسی به داده‌های مورد نیاز.

کنترلهای کاربردی فناوری اطلاعات، روشهای دستی یا

خودکاری است که به‌طور معمول در سطح فرایندهای تجاری اجرا می‌شود و برای پردازش معاملات به‌وسیله نرم‌افزارهای کاربردی به‌کار می‌رود. کنترلهای کاربردی می‌تواند ماهیت پیشگیری‌کنندگی یا کشف‌کنندگی داشته باشد و برای به‌دست‌آوردن اطمینان از درستی سوابق حسابداری طراحی می‌شود. از اینرو، کنترلهای کاربردی به روشهای مورد استفاده در انجام، ثبت، پردازش و گزارش معاملات یا دیگر اطلاعات مالی مربوط می‌شود. به کمک این کنترلها اطمینان به‌دست می‌آید که معاملات انجام‌شده، به تصویب رسیده و به‌طور کامل و درست ثبت و پردازش شده‌اند."

همانطور که مشخص است، خطرهایی که در یک واحد تجاری از طریق طراحی و اجرای کنترلهای عمومی فناوری اطلاعات، کنترل و مدیریت می‌شوند، تأثیر درخور ملاحظه‌ای بر اثربخشی حسابرسی و در نتیجه بر ریسک حسابرسی دارند و از اینرو باید مورد شناخت و ارزیابی از سوی حسابرس قرار گیرند.

حسابرسان هنگام اجرای حسابرسی درمحیطهای وابسته به سیستمهای اطلاعاتی مبتنی بر فناوری اطلاعات باید دامنه مناسبی از حسابرسی فناوری اطلاعات را تعیین و به‌مرحله اجرا درآورند

طی دو دهه اخیر، واحدهای تجاری در پی تغییرهای فناوری، رقابت، الزامات قانونی و حتی تغییرها در هدفهای استراتژیک خود، سرمایه‌گذاریهای درخور ملاحظه‌ای، در بعضی موارد میلیارد تومانی، برای گسترش بهره‌مندی از فناوری اطلاعات، به‌خصوص در بخش نرم‌افزارهای کاربردی داشته‌اند. همانطور که می‌دانید، نرم‌افزار کاربردی یا سیستم نرم‌افزاری، نوعی نرم‌افزار است که کاربران را قادر می‌سازد در انجام وظایف خود قابلیتهای کامپیوتر را به خدمت بگیرند. بر پایه طبقه‌بندی انجام‌شده از سوی انجمن بین‌المللی حسابرسان داخلی، این نوع سیستمها در دو گروه **نرم‌افزارهای ثبت‌وضبط** (Transactional Applications) و **نرم افزارهای پشتیبانی** (Support Applications) قابل طبقه‌بندی هستند. نرم‌افزارهای ثبت وضبط، تسهیلات لازم برای فراوری داده‌ها در همه ابعاد سازمان را از راههای زیر فراهم می‌کند:

- ثبت بهای مبادلات تجاری در قالب واژه‌های بدهکار و بستانکار،
- ایجاد مخازنی برای داده‌های مالی، عملیاتی و انتظام‌بخشی، و
- میسرسازی تهیه انواع گزارشهای مالی و مدیریتی و عملیاتی برای تمامی فرایندها.

این سیستمها در شکلهای گوناگون مانند سیستمهای تک‌موضوعی (سیستم حقوق و دستمزد، سیستم حسابداری و...)، **سیستمهای اطلاعات مدیریت** (MIS)، **سیستمهای یکپارچه / جامع** (Integrated/Total Systems)، سیستمهای **برنامه‌ریزی منابع بنگاه** (ERP) و... از سوی تولیدکنندگان مختلف تهیه و عرضه می‌شوند و حتی در مواردی طراحی و تولید تمامی اجزای این سیستمها و یا بخشهایی از آنها به‌طور مستقیم در واحد تجاری استفاده‌کننده انجام می‌شود. این سیستمها مبادلات و بده‌بستانها را بر پایه منطق برنامه‌نویسی‌شده که در بسیاری موارد مبتنی بر قواعد

تجـاری انحصـاری حاکم بـر عملیات و فرایندهای شـرکت یا سازمان بهره‌بردار است مورد پردازش قرار می‌دهند.

نرم‌افزارهای پشتیبانی، برنامه‌های نرم‌افزاری با کاربردهای مشـخصی هسـتند که بـرای آسـان‌کردن اجـرای فعالیتهای کسب‌وکار مورد بهره‌برداری قرار می‌گیرند. از متعارف‌ترین این برنامه‌ها، برنامه متن‌پرداز، نرم‌افزار ارسال و دریافت **نامه‌های الکترونیکـی** (E-mail)، نرم‌افـزار **نمابـر** (Fax)، نرم‌افزار **تصویربرداری از اسناد و مدارک** (Scan)، نرم‌افزار **طراحی و مدل‌سـازی**(Design) و نرم‌افزار **ارائه** (Presentation) هسـتند. همانطور که می‌دانید، این نرم‌افزارها به‌طور عمومی نقشی در پردازش اطلاعات ایفا نمی‌کنند.

در کنـار ریسـکهای ذاتی فرایندهـای تجـاری، نرم‌افزارهای ثبت‌وضبط و نرم‌افزارهای پشتیبانی، با هر فناوری که تولید شده باشند، ممکن است سازمان را با ریسکهای ناشی از خصوصیات ذاتـی آن فنـاوری و نحـوه **پیکربنـدی** (Configuration)، **راهبری** (Manage) و اسـتفاده کارکنان از سیستم، مواجه کنند که در صورت نبود اقدام مناسـب برای تخفیف آثار این ریسکها، یکدسـتی، کامـل بـودن، به‌جـا بـودن و در دسـترس بـودن اطلاعـات مالی و عملیاتی ممکن اسـت تحـت تأثیرات منفی قـرار گیـرد. در همین راسـتا، بسـیاری از سـازمانهای آگاه به پیامدهای بی‌توجهی به ریسـکها، ترکیبی از **کنترلهای دستی** (Manual) و **خـودکار**(Automated) را بـرای مدیریـت ریسکهای ناشـی از نرم‌افزارهای ثبت‌وضبط و پشتیبانی مورد توجه قرار می‌دهند.

به‌طور کلی، میزان موفقیت در مدیریت ریسک نرم‌افزارهای مورد اسـتفاده، تابع سـطح مدارا با ریسک و یا **سطح اشتیاق ریسـک** (Risk Appetite) در سـازمان، درجه بلوغ ارزیابی ریسـک در حوزه کاربردی نرم‌افزار مورد بررسـی، فرایندهای تجاری متأثر از ریسـک، اثربخشی کنترلهای عمومی فناوری اطلاعـات و بالأخـره، میزان اثربخشـی کنترلهـای کاربردی فناوری اطلاعات است.

همانطور که در ابتدا اشاره شـد، کنترلهای کاربردی فناوری اطلاعـات عبـارت از روشـهای دسـتی یا خودکاری اسـت که به‌طـور معمـول در سـطح فرایندهای تجاری اجرا می‌شـود و برای پردازش معاملات به‌وسـیله نرم‌افزارهای کاربردی به‌کار می‌رود. این کنترلها برای اطمینان از موارد زیر هستند:

- داده وارده به سیسـتم، دقیق، کامل، مجاز و غلط‌گیری شده است،
- داده در مدت زمان قابل‌قبول تحت پردازشـهای مد نظر قرار می‌گیرد،
- داده ذخیره‌شده، صحیح و کامل است،
- خروجیها صحیح و کامل هستند، و
- سـابقه قابل ردیابی جریان داده از هنگام ورود تا ذخیره‌سازی و خروج احتمالـی (حذف داده)، در قالب یک رکورد اطلاعاتی وجود دارد.

انواع مختلـف کنترلهای کاربردی برای دسـتیابی به هدفهای یادشده عبارتند از:

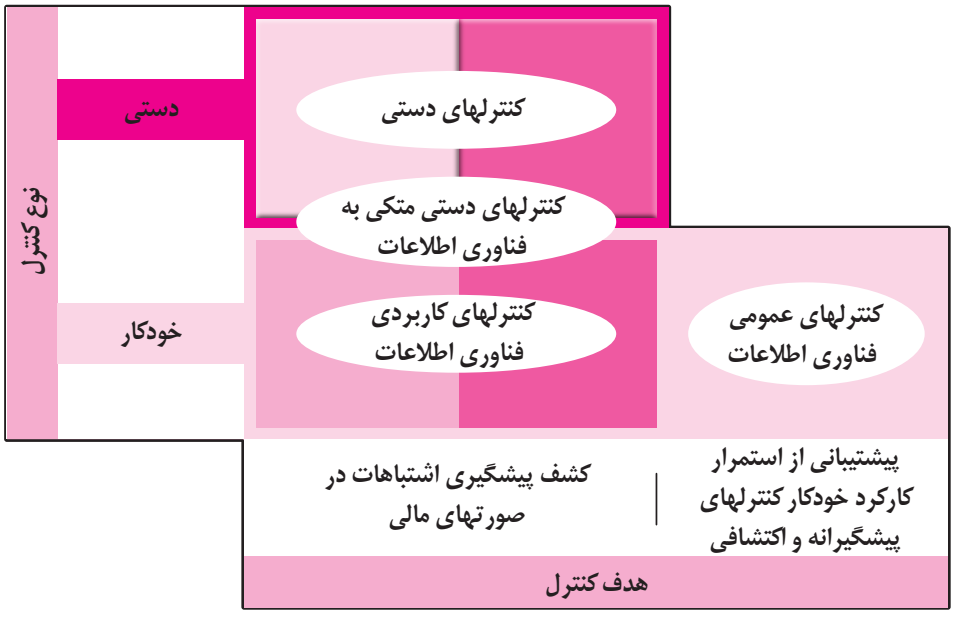
- **کنترلهای ورودی**: هدف اصلی این کنترلها، وارسی بی‌عیبی داده‌های واردشـده به نرم‌افزار است. داده ممکن است به‌طور مستقیم به‌وسیله کارکنان یا از سوی یک شریک تجاری و یا از طریق یک صفحه اینترنتی به سیستم وارد شده باشد، ولی در هر حال مورد وارسی قرار می‌گیرد تا از انطباق آن با ویژگیهای از پیش تعریف‌شده اطمینان حاصل شود.
- **کنترلهای پردازشـی**: این کنترلهـا تأمین‌کننده پیامی خودکار مبنی بر انجام کامل، بی‌عیب و مجاز پردازش در سیستم هستند.
- **کنترلهای خروجی**: این کنترلها مبتنی بر کارهای انجام‌شده بر روی داده هسـتند و باید نتایج حاصل از اجرای آنها بر روی داده‌های ورودی با خروجیهای مورد انتظار مقایسه شود.
- **کنترلهـای یکپارچگـی**: هدف از این کنترلهـا پایش فرایند پـردازش و ذخیره‌سـازی داده به‌منظـور اطمینـان از حفـظ سازگاری و درستی داده در سیستم است.
- **پی‌جویی مدیریت**: کنترلهای تاریخچه پردازشـها اسـت، که بیشـتر اوقات به‌عنـوان پی‌جویی یا **رد پای حسابرسـی** (Audit Trail) نیز شناخته می‌شود. این کنترلها به مدیریت امـکان می‌دهد موارد تبادل داده‌ها و رویدادهای واقع‌شـده در جریـان پردازشـها را از طریـق ثبـت خودکارجزئیـات وقایع از سرچشـمه تا نتیجه را شناسایی و به‌طور معکوس ردیابی کند. این کنترلها همچنین اثربخشی دیگر کنترلها را پایش می‌کند و نزدیکترین منشأ خطاها را شناسایی می‌نماید.

از مؤلفه‌های کنترلهای کاربردی، پیشگیرانه یا اکتشافی‌بودن

آنها است. اگرچه هر دو نوع این کنترلها بر پایه منطق برنامه‌ریزی‌شده یا پیکربندی سیستم عمل می‌کنند، کنترل پیشگیرانه، همانگونه که از نام آن مشخص است، مانع بروز خطا در نرم‌افزار کاربردی می‌شود. روال اعتبارسنجی یا تأیید **داده ورودی** (Data Validation)، نمونه‌ای از این کنترل است. از سوی دیگر کنترل اکتشافی، خطاها را بر پایه منطق از پیش تعریف‌شده در برنامه شناسایی می‌کند. نمونه‌ای از این نوع کنترل، مقایسه یک **عنصر داده‌ای**(Data Element) در **سابقه** (Record) موجودیت داده‌ای با عنصر داده‌ای متناظر در سابقه موجودیت داده‌ای دیگر است (برای مثال، نرخ منعکس در سابقه اطلاعاتی صورتحساب فروشنده در مقایسه با نرخ خرید منعکس در سابقه سفارش خرید مربوط به آن). کنترلهای کاربردی خودکار، به‌ویژه آنهایی که دارای ماهیت اکتشافی هستند، در پشتیبانی کنترلهای دستی نیز نقشی اساسی ایفا می‌کنند. شاخص‌ترین نمونه، استفاده از داده یا نتایج کنترل اکتشافی در اعمال نظارتهای دستی بر امور است. به‌عنوان مثال، برای جلب توجه به موارد مغایرت نرخ موضوع مثال قبل، می‌توان گزارشی از مغایرتها تهیه کرد تا برای بررسی و تعیین اقدامات کنترلی لازم در اختیار مدیریت قرار گیرد. **شکل ۱** ارتباط کنترلهایی راکه تا اینجا مرور کردیم به‌خوبی نشان می‌دهد.

توجه به این نکته ضروری است که میزان اتکا به کنترلهای کاربردی، رابطه مستقیم با تناسب طراحی و اجرای اثربخش کنترلهای عمومی دارد. برای مثال، چنانچه کنترلهای عمومی که برای پایش تغییرات برنامه‌های کاربردی در نظر گرفته شده به هر دلیل اثربخش نباشد، ممکن است تغییراتی غیرمجاز، تأییدنشده و آزمون‌نشده در نرم‌افزارهای کاربردی صورت گیرد که منجر به از بین رفتن یکپارچگی کنترلهای کاربردی و بی‌اثر بودن آنها شود. موارد زیر از جمله مهمترین عوامل تأثیرگذار بر میزان اتکا به کنترلهای کاربردی فناوری اطلاعات شناخته شده‌اند:

- میزان تفکیک وظایف (درسطح دسترسی به نرم‌افزارها و در سطح دسترسی به امکانات نرم‌افزارها)،
- میزان زیرپا گذاری کنترلها (چه کسانی می‌توانند کنترلها را زیرپا گذارند و چگونه این امر پایش می‌شود)،
- میزان وابستگی کنترلها به یکدیگر،
- میزان امنیت دسترسی به پرونده‌های اصلی داده‌ها و چگونگی کنترل تغییرات پرونده‌های اصلی،
- ارتباطات سیستمها (چگونگی جریان داده‌ها و کنترلهای نظارتی بر عملکرد مؤثر و به‌هنگام کانالهای ارتباطی)،
- نظارت بر عملیات **دسته‌ای** (Batch)، اینکه چه کنترلهایی متأثر از عملیات دسته‌ای هستند و عملیات دسته‌ای چگونه پایش می‌شوند)، و

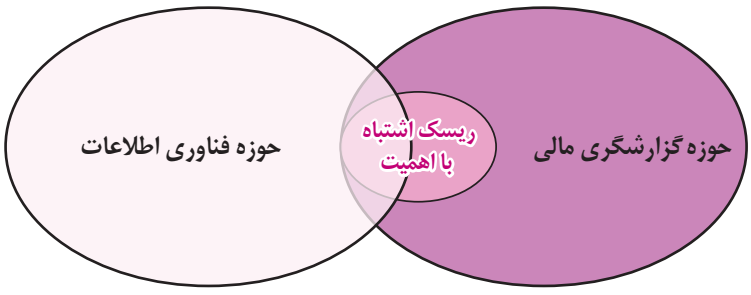


شکل ۱ - کنترلهای فناوری اطلاعات

• ضعفهای کنترلهای عمومی فناوری اطلاعات.

بسیار خوب، اجازه بدهید ادامه مطلب را با پرداختن به دامنه حسابرسی فناوری اطلاعات در حسابرسی صورتهای مالی ادامه بدهیم. لطفاً به **شکل ۲** توجه کنید. همانطور که اطلاع دارید، **حسابرسی فناوری اطلاعات** (IT Audit) شاخه‌ای مستقل از حسابرسی صورتهای مالی است. حسابرسان فناوری اطلاعات، اجزا و ابعاد گوناگون فناوری اطلاعات در یک سازمان را مورد حسابرسی قرار می‌دهند. هرچه دامنه استفاده از فناوری اطلاعات در یک سازمان گسترده‌تر باشد، حوزه‌های کاری حسابرسان فناوری اطلاعات گسترده‌تر می‌شود. با توجه به تأثیر فناوری اطلاعات بر نحوه اعمال فعالیتهای کنترلی، استاندارد حسابرسی ۳۱۵، حسابرسان را ملزم به کسب شناخت از روشهای کنترلی سیستمهای فناوری اطلاعات نسبت به عملیات شناسایی، ثبت، پردازش، اصلاح و گزارشگری اطلاعات مربوط به معاملات دانسته است و در جایی که مستنداتی درباره معاملات به جز آنچه به‌وسیله سیستم فناوری اطلاعات ایجاد می‌شود وجود نداشته باشد، اجرای آزمون کنترلها در ارتباط با کنترلهای فناوری اطلاعات را اجتناب‌ناپذیر اعلام کرده است. در اینجا این پرسش پیش می‌آید که به‌منظور اجرای الزامات یادشده، آیا حسابرسان صورتهای مالی باید از دانش و مهارتهای حسابرسان فناوری اطلاعات برخوردار باشند؟ پاسخ این است که حسابرسان صورتهای مالی یا باید خود از دانش و مهارتهای لازم برای حسابرسی حوزه‌هایی از فناوری اطلاعات که مرتبط و مربوط به 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 مبتنی‌بر ریسک باید مد نظر قرار گیرد.

برای این منظور ابتدا باید دامنه گزارشگری مالی مشخص شود (**شکل ۲**) و با در نظر داشتن محدوده یادشده به پرسشهای زیر پاسخ داده شود:



شکل ۲- ارتباط حسابرسی فناوری اطلاعات و حسابرسی صورتهای مالی

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

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

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

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 ۲** مشخص است، تنها بخشی از حوزه فناوری اطلاعات به فرایند گزارشگری مالی مربوط است و کنترلهای آن به‌عنوان کنترلهای مرتبط

بـا حسابرسـی صورتهای مالی (طبـق تعریف اسـتاندارد ۳۱۵ حسابرسـی) در نظر گرفته می‌شـود، پس این بخش باید مورد شناخت و در صورت ضرورت مورد ارزیابی حسابرس قرار گیرد. اجزای این بخش در عمل می‌تواند شـامل روشهای گردآوری، پردازش، ذخیره‌سازی و انتقال داده‌ها باشد.

طبق استاندارد حسابرسـی ۳۱۵، فرایند کسب شناخت باید به‌نحوی انجام شـود که حسابرس را قادر به تشخیص و براورد خطرهـای تحریف بااهمیت که متشـکل از خطـر ذاتی و خطر کنترل اسـت کند. در محیطهای بهره‌مند از فناوری اطلاعات، خطر کنترل وابستگی زیادی به فناوری اطلاعات دارد؛ از اینرو تعیین ریسکهای ناشی از کنترلهای فناوری اطلاعات و از میان آنها شناسـایی ریسکهایی که ممکن است اشتباههای بااهمیت در صورتهـای مالی ایجاد کنند، امری اجتناب‌ناپذیر اسـت. در چنین محیطهایی، ریسک ذاتی در سطح کلیت صورتهای مالی شامل ریسک کنترلهای عمومی فناوری اطلاعات نیز می‌شود.

به‌عنوان مثال، فرض کنید حسـابرس (کارشـناس حسابرسی فنـاوری اطلاعات) نسـبت به تناسـب و عملکرد **دیـوار آتش** (Firewall) در سیسـتمهای واحـد مورد رسـیدگی که از جمله کنترلهای عمومی برای ایجاد امنیت هنگام ارتباط با شـبکه‌های بیرونی اسـت، اطمینان لازم را حاصل نکند. در چنین شرایطی چنانچـه سیسـتمهای مرتبط با حـوزه گزارشـگری مالی، تحت همان شبکه‌ای اجرا شوند که با شبکه بیرونی ارتباط برقرار کرده، احتمال تهدیدهای سـایبری نسـبت به آنها تشدید می‌شود و لذا ریسک ذاتی در سطح کلیت صورتهای مالی به‌شدت افزایش پیدا می‌کنـد. البته نباید از نظر دور داشـت که در عین وجود ریسـک فـوق، چنانچه **کنترلهای دسترسـی** (Access Controls) و دیگر کنترلهای عمومی و کاربردی پیرامون داده‌های گزارشگری مالی و فرایندهای تهیه گزارشـها به‌خوبی طراحی شـده باشـد و نتایج آزمون آنها دلالت بر اثربخشی کنترلها داشته باشد، ریسک ناشی از کنترل دیوار آتش در دامنه ریسک اشتباه بااهمیت (حلقه کوچک در **شکل ۲**) قرار نخواهد گرفت و لذا ارزیابی آن می‌تواند ضرورت پیدا نکند.

برپایه آنچه ارائه شد، حسابرسان هنگام اجرای حسابرسی در محیطهای وابسـته به سیستمهای اطلاعاتی مبتنی بر فناوری اطلاعات باید دامنه مناسـبی از حسابرسـی فناوری اطلاعات را تعییـن و بـه مرحلـه اجـرا درآورند. ایـن دامنه تحـت تأثیر میزان فصل مشـترک حوزه گزارشـگری مالی با حوزه فناوری اطلاعـات واحـد مـورد رسـیدگی و همچنین فصل مشـترک محـدوده ریسـکهای اشـتباههای بااهمیت با حـوزه فناوری اطلاعات تعیین می‌شود(محل تقارن حلقه‌ها در **شکل ۲**).

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 اسـت. یک سـازمان کوچک ۵۰ نفری که برای توزیع محصولات یا خدمات، برای اعلام داده‌های حقوق کارکنان به بانک و برای دسترسی **برخط** (Online) مدیران به اطلاعات گـردش عملیات برای اداره امور شـرکت از فنـاوری اطلاعات اسـتفاده می‌کنـد، در نهایـت متکـی بـه کنترلهـای فنـاوری اطلاعات در فرایندهای گزارشـگری مالی اسـت، در سطحی متوسـط به بالا از کمال فناوری اطلاعات طبقه‌بندی می‌شود. در نقطه مقابل، کارخانه‌ای با انبارهای متعدد و هزاران مشتری و صدهـا کارگر، ولی متکی به نرم‌افزارهای تجاری گوناگون که برای تهیه گزارشـهای مالی به یک **سرویس دهنده** (Serv-er) متصل شده‌اند، درسطحی پایین از کمال فناوری اطلاعات قرار دارد.

هرچه سـطح کمـال فناوری اطلاعـات در سـازمان پایینتر باشـد، حوزه فناوری اطلاعات در آن سازمان کوچکتر و دامنه کار حسابرسـی فناوری اطلاعات برای حسابرسـان صورتهای مالی محدودتر خواهد بود و بالعکس.

به‌نظر شـما بانکهـای ما در چه سـطحی از کمـال فناوری اطلاعات قرار دارند؟

موفق باشید

منابع:

- **استانداردهای حسابرسی ایران**، سازمان حسابرسی، ۱۳۹۱
- **Auditing Application Controls**, IIA, 2007
- **The Minimum IT Controls to Assess in a Financial Audit**, ISACA Journal , Volume 1, 2010.
- **What Every IT Auditor Should Know About Scoping an IT Audit**, ISACA Journal, Volume 4, 2009