دامنه حسابرسی فناوری اطلاعات

نیوشا ابراهیمی*

پیشگفتار

حسابرسان فناوری اطلاعات، به‌عنوان بخشی از کارکرد حسابرسی داخلی، محتویات سبد فناوری اطلاعات[1] واحد تجاری را حسابرسی می‌کنند. هرچه واحد تجاری بزرگتر باشد، فضای فناوری اطلاعات آن گوناگون‌تر و جالب‌تر است و حسابرس فناوری اطلاعات می‌تواند حسابرسی‌های متنوع‌تری را اجرا کند. فضای فناوری اطلاعات، به همه اجزای فناوری اطلاعات در واحدهای تجاری، اطلاق می‌شود و تمام این اجزا و سامانه‌ها را در واحد تجاری، پوشش می‌دهد. حسابرسان فناوری اطلاعات به‌عنوان کارکنان موسسات حسابرسی، بخشی از فضای فناوری اطلاعات مرتبط با گزارشگری مالی را در گستره متنوعی از کسب‌وکار، حسابرسی می‌کنند که باید جالب و به‌گونه‌ای انکارناپذیر، تجربه بزرگی باشد. این کار برای شرکت‌های سهامی عام، در برگیرنده حسابرسی‌های کنترل‌های مربوط به بخش ٤٠٤ قانون ساربینز-اکسلی[2] و برای همه واحدهای تجاری نیازمند حسابرسی‌های مالی، دربرگیرنده حسابرسی‌های کنترل‌های فناوری اطلاعات ناظر بر گزارشگری مالی است. همچنین در جایی‌که هدف به‌طور مستقیم مبارزه با جرم‌ها یا اعمال بالقوه مجرمانه است، حسابرس فناوری اطلاعات می‌تواند به‌عنوان متخصص جرایم رایانه‌ای (سایبری) [3] به‌کار گمارده شود، برای نمونه، متخصصان جرایم سایبری ممکن است در جستجوی شواهد دیجیتال، برای موسسه حسابرسی یا موسسه حسابرسی جرایم رایانه‌ای کار کنند و مسئولیت بررسی موارد ارتکاب تقلب را برعهده بگیرند. یا اینکه، متخصص جرایم سایبری همان کار را برای دولت یا سازمان مجری قانون انجام دهد، برای نمونه، در این مورد، دفتر تحقیقات دولت مرکزی آمریکا[4] و دفتر بازرسی کل

آمریکا[5]، همواره چنین متخصصانی را به‌کار می‌گمارند. البته، راه‌های متنوع دیگری نیز برای به‌کارگیری مهارت‌ها، دانش و توانمندی‌های مرتبط با حسابرسی فناوری اطلاعات شامل مشاوره و مدیریت اجرایی (برای نمونه، مدیر ارشد فناوری اطلاعات[6]) وجود دارد.

این نوشتار بر تفاوت‌های موجود در دامنه فناوری اطلاعات میان دو دیدگاه نخست تاکید دارد و به‌ویژه، از دیدگاه حسابرسان مستقل به موضوع حسابرسی فناوری اطلاعات می‌نگرد. از دردسرهای حسابرسان تازه‌کار فناوری اطلاعات، این است که تفاوت میان حسابرسی فناوری اطلاعات در حسابرسی مالی را در برابر حسابرسی فناوری اطلاعات از دیدگاه فناوری اطلاعات (به‌طور معمول، از جنبه کارکرد حسابرسی داخلی یا مشاوره)، تشخیص نمی‌دهند و این کار به‌طور معمول با روندی فزاینده منجر به تعیین دامنه فناوری اطلاعات نامناسب در حسابرسی مالی می‌شود.

به‌کارگیری اصول و روش‌های حسابرسی فناوری اطلاعات

دشواری در تعیین دامنه فناوری اطلاعات در حسابرسی مستقل، ناشی از این واقعیت است که حسابرس فناوری اطلاعات، نیاز دارد تا از فضای فناوری اطلاعات و اجزای آن بسیار بداند. این فضا دربرگیرنده فهرست مناسبی از راهکارهای برتر[7]، محک‌ها[8]، بیانیه‌های مدون و مدل‌های مرتبط با هر یک از آن اجزا و دانش کافی پیرامون فناوری‌های گوناگون (مانند، نیاز به متخصص شدن در زمینه رایانه‌ها و فناوری‌ها) است. حسابرسان فناوری اطلاعات پیرامون چرخه حیات گسترش سامانه‌ها[9]، راهبری فناوری اطلاعات، مدیریت پروژه، کنترل‌های دسترسی/ کنترل‌های عمومی فناوری اطلاعات[10]، شبکه‌ها، نرم‌افزار و استمرار کسب‌وکار (بازیابی اطلاعات در هنگام بروز پیشامدهای ناگوار) کاربلد هستند. حسابرسان فناوری اطلاعات در موارد پیشگفته، باید همه مراحل یا محک‌های چندگانه نیازمند آزمون را مانند موارد زیر بدانند:

- برنامه مدون،
- واگذاری وظایف،
- ذخیره‌سازی (انبارش) از نسخه‌های پشتیبان اطلاعات در خارج از سایت مربوط،
- پشتیبان‌گیری از امکانات سامانه،
- پشتیبان‌گیری از منابع،
- پشتیبان‌گیری از سامانه‌عامل[11]،
- پشتیبان‌گیری از برنامه کاربردی،
- رتبه‌بندی فرامین اجرای بازذخیره (باز انبارش) برنامه‌های کاربردی و داده‌ها،
- رونوشت‌های رهنمودهای فنی،
- آزمون برنامه، و
- مستندسازی آزمون.

حسابرسان فناوری اطلاعات عموما برای اجرای روش‌های مرتبط با راهکارهای برتر مانند موارد زیر در حسابرسی فناوری اطلاعات از دیدگاه فناوری اطلاعات، آموزش دیده‌اند:

- بررسی مستندات (برنامه، واگذاری کار، آزمون نتیجه‌ها و موارد دیگر)،
- پرس و جو از کارکنان کلیدی،
- باز اجرا (باز انبارش) داده‌ها، و
- بررسی و تایید امکانات پشتیبان‌گیری، منابع، رهنمودهای فنی، سامانه‌عامل، برنامه‌های کاربردی و موارد دیگر.

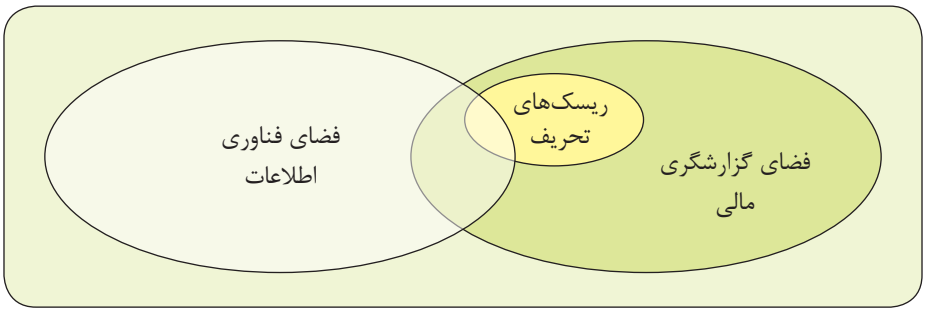
اگر کار انجام شده به صورت حسابرسی در زمینه فناوری اطلاعات، حسابرسی داخلی یا مشاوره باشد و فرض شود که واحد تجاری، دارای فضای فناوری اطلاعات بزرگ یا بسیار پیچیده است، مجموعه کامل بیان شده در مورد موضوعات پیشگفته، در این نوع حسابرسی، کاربرد دارد. چنین مواردی برای حسابرسی‌های فناوری اطلاعات پیرامون کارافزارهای مجازی[12]، امنیت اطلاعات و گروهی از دیگر مولفه‌ها یا اجزای فضای فناوری اطلاعات، به‌کار می‌رود. حسابرسان فناوری اطلاعات از این موضوع آگاهند که راهنمای کوبیت (هدف کنترل برای اطلاعات و فناوری‌های مرتبط)[13] منتشر شده از سوی انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی[14]، مدل و ابزاری پیشرو برای یاری‌رسانی به حسابرسان فناوری اطلاعات در این نوع حسابرسی‌ها، را ارایه کرده است. اما اگر زمینه کار، حسابرسی مالی باشد، چه روی می‌دهد؟ آیا در واقع چیزی تغییر می‌یابد؟

به‌کارگیری اصول حسابرسی مبتنی‌بر ریسک

همواره حسابرسان فناوری اطلاعات در حسابرسی مالی فریفته می‌شوند و خواهان به‌کارگیری تمام دانش سودمند خود در اجرای حسابرسی‌ها هستند. اگر حسابرسان فناوری اطلاعات مراقب نباشند، کار را به حد افراط (برای نمونه، اجرای روش‌ها و آزمون‌های نسبتا بیشمار) انجام می‌دهند. زیرا ماهیت کار حسابرسان فناوری اطلاعات اینگونه است که در به‌کارگیری دانش و مهارت‌های ویژه خود دقیق باشند. حسابرسان فناوری اطلاعات، گاهی با تعیین دامنه مناسب پیرامون بخش حسابرسی فناوری اطلاعات از حسابرسی مالی، مبارزه می‌کنند و تشخیص نمی‌دهند که مجموعه‌ای از روش‌های بیشمار را گسترش می‌دهند. روشی هوشمندانه برای اطمینان از کم و زیاد نبودن دامنه مناسب، این است که به‌جای اتکای صِرف بر بیانیه‌های مدون یا راهکارهای برتر در آن حوزه، بر اصول حسابرسی مبتنی‌بر ریسک۱۵ اتکا شود.

حسابرسی مبتنی‌بر ریسک همانگونه

نمایه شماره ۱- تعیین دامنه حسابرسی فناوری اطلاعات در حسابرسی مالی



که در نمایه شماره یک مشاهده می‌شود با تعریف فضای گزارشگری مالی آغاز می‌شود چه رهنمود و سامانه‌های خودکاری در گزارشگری مالی به‌کار گرفته شده است؟ کدام حساب‌ها، طبقه معاملات و موارد افشای اطلاعات به گزارشگری مالی مربوط است؟ چه فرایندها، رهنمودها و موارد خودکارسازی شده در گزارشگری مالی اجرا شده است؟

بنابراین، در این باره برای تعیین دقیق اجزای مرتبط، لازم است فضای فناوری اطلاعات مورد ارزیابی قرار گیرد. این کار می‌تواند برای آغاز حسابرسی بدون کوشش وظیفه‌شناسانه برای آزمون و تعریف فضای مرتبط با فناوری اطلاعات، وسوسه‌انگیز باشد و حسابرسی فناوری اطلاعات تنها بر پایه برخی مفروضات دیگر (عرف، روش‌های حسابرسی پیشین، قضاوت حرفه‌ای و....) اجرا شود. واقعیت این است که تمام فضای فناوری اطلاعات، به حسابرسی مالی مربوط نمی‌شود. تنها بخش فضای فناوری اطلاعات که با حسابرسی مالی پیوند دارد، بخشی است که با فضای گزارشگری مالی همپوشانی[16] دارد (در نمایه شماره ۱ دیده می‌شود که در آن دو دایره وِن[17] با یکدیگر همپوشانی دارند). از دیدگاه عملی، این مورد، دستیابی به شناخت از تمام داده‌های مرتبط با گزارشگری مالی و همه داده‌های فناوری اطلاعات پیرامون دریافت، پردازش، ذخیره‌سازی (انبارش) یا انتقال آن داده‌ها را دربر می‌گیرد، به این معنی که این اجزا، مربوط خواهند بود.

> دشواری در تعیین دامنه فناوری اطلاعات در حسابرسی مستقل، ناشی از این واقعیت است که حسابرس فناوری اطلاعات، نیاز دارد تا از فضای فناوری اطلاعات و اجزای آن بسیار بداند

اما این کار، تنها نخستین گام دشوار در تعیین دامنه فناوری اطلاعات مناسب در حسابرسی مالی است. برای گام دوم، این همپوشانی از راه ریسک تحریف‌های بااهمیت[18] محدود می‌شود. ریسک تحریف‌های بااهمیت در استانداردهای مبتنی‌بر ریسک انجمن حسابداران رسمی آمریکا [19] برای غیرناشران تعریف شده است و به اصول مندرج در آن با عنوان حسابرسی مبتنی‌بر ریسک اشاره می‌شود. ریسک تحریف‌های بااهمیت دربرگیرنده ریسک کنترل[20] مرتبط با فناوری اطلاعات و ریسک ذاتی[21] مربوط به واحد تجاری به اشکال گوناگون است (برای نمونه، کنترل‌های عمومی فناوری اطلاعات). اساسا، حسابرسان فناوری اطلاعات مسئولیتی دو چندان پیرامون این موارد دارند:

۱- تعیین اینکه چه ریسک‌هایی به‌عنوان پیامدی ناشی از تاثیر فناوری اطلاعات بر گزارشگری مالی وجود دارد، و

۲- شناسایی ریسک‌های (برای نمونه، ریسک تحریف‌های بااهمیت) مرتبط با کنترل‌های جاسازی شده در فناوری اطلاعات.

اگر واحد تجاری، برنامه‌های کاربردی نرم‌افزاری خود را ایجاد کند و یکی از آن برنامه‌های کاربردی، گزارش‌های مالی را پردازش می‌کند، پس، ریسک موجود در گزارشگری مالی به‌عنوان پیامدی از چیزی در فضای فناوری اطلاعات پدید می‌آید و آن، ایجاد این برنامه‌های کاربردی نرم‌افزاری است.

اما این پرسش پیش می‌آید که آیا این ریسک، مربوط است؟ اگر ریسک موجود به‌سوی ریسک تحریف‌های بااهمیت حرکت کند، مربوط به‌شمار می‌آید. اگر به آن سو حرکت نکند، نامربوط به‌شمار می‌آید. برای نمونه، هنگامی که سامانه‌های داخلی به درگاهی[22] ارتباط داده شده باشند که به‌سوی اینترنت هدایت می‌شود، حسابرسان فناوری اطلاعات بر دیوارهای آتش[23] تمرکز می‌کنند. چون سامانه‌های مرتبط با گزارشگری مالی به اینترنت ارتباط داده شده است، این بخش از فضای فناوری اطلاعات با فضای گزارشگری مالی همپوشانی دارد. اما اگر کنترل‌های دسترسی و کنترل‌های دیگری پیرامون داده‌های گزارشگری مالی وجود داشته که آزمون شده باشد و دریافته شود که نسبت

به درستی آنها اطمینان مناسب فراهم شده است، بررسی دیوارهای آتش، نامربوط به‌شمار می‌آید و نیازی به آزمون ندارند (به این معنی که اگرچه در نخستین همپوشانی قرار می‌گیرند، اما در همپوشانی ریسک تحریف‌های بااهمیت قرار نمی‌گیرند). اگر کنترل‌های دسترسی درستی (کنترل‌های کاربردی یا کنترل‌های دسترسی) در لایه بالایی داده‌های گزارشگری مالی وجود داشته باشد، بسیاری از موارد در این محدوده، نامربوط به‌شمار می‌آید. بنابراین، آنچه پس از همپوشانی فضای فناوری اطلاعات و فضای گزارشگری مالی درنظر گرفته می‌شود، همپوشانی فضای ریسک تحریف‌های بااهمیت است. این همپوشانی براساس سطحی از ریسک مرتبط با فضای فناوری اطلاعات و ریسک تحریف‌های بااهمیت در فضای گزارشگری مالی پایه‌ریزی شده است (برای نمونه، این کار می‌تواند به‌سوی تحریف‌های بااهمیت حرکت کند یا راه دیگری در پیش گرفته شود که دارای سطح بالای ارزیابی ریسک باشد).

در حسابرسی مبتنی‌بر ریسک، به حسابرس فناوری اطلاعاتی نیاز است که سطحی مناسب از (دربرگیری) فضای فرعی در برنامه حسابرسی مالی را درنظر بگیرد تا بتواند به‌سوی کاهش در آن میزانی حرکت کند که مربوط به‌شمار آید. این کاهش در جزء فضای فناوری اطلاعات، با حسابرسی فناوری اطلاعات از دیدگاه فناوری اطلاعات، بسیار متفاوت است. در این مورد، یکی، تمام فضای فرعی مربوط به هدف را دربر می‌گیرد.

یک موضوع بااهمیت دیگر درباره نمایش وِن و تعیین دامنه فناوری اطلاعات مناسب، موضوع تعیین دامنه برپایه تکامل[۲۴] فناوری اطلاعات است[۲۵]. با تکامل‌یافته‌تر شدن فضای فناوری اطلاعات، اندازه حلقه یا فضای همپوشانی میان فضای گزارشگری مالی و فضای فناوری اطلاعات بزرگتر خواهد بود، به این معنی که هرچه همپوشانی بزرگتر باشد، دامنه بزرگتری از روش‌های فناوری اطلاعات لازم است و برعکس.

نمونه

برای نمونه، دو سناریو در نظر گرفته می‌شود در سناریوی اول، در کسب‌وکاری متوسط، برنامه نرم‌افزاری مایکروسافت داینامیکس[۲۶] با تعدادی سِرور به‌کار گرفته شود و این کسب‌وکار از درآمدی برابر با[۲۵] میلیون دلار برخوردار باشد، سناریوی دوم، مربوط به شرکت کوکاکولا است، این شرکت جهانی، سامانه برنامه‌ریزی منابع بنگاه[۲۷] را به‌کار گرفته و درآمدی میلیارد دلاری دارد.

در سناریوی نخست، حسابرس فناوری اطلاعات نیازی به کوشش بسیار برای آزمون نرم‌افزار ندارد، زیرا واحد تجاری، نرم‌افزار تجاری دارد که سال‌هاست آن را به‌کار گرفته است. در بیشتر موارد، حسابرس فناوری اطلاعات باید ببیند که نسخه‌ای نسبتا بهنگام از نرم‌افزار، به‌کار گرفته شده باشد. در سناریوی دوم، هرچند در شرکت کوکاکولا، نرم‌افزار تجاری به‌کار گرفته شده است، به احتمال بیشتر، این سطح تکامل، برخی سطوح ریسک مرتبط با نرم‌افزار را پدید می‌آورد که از سناریوی نخست بزرگتر است. بنابراین، بیشتر احتمال می‌رود که حسابرس فناوری اطلاعات، برخی آزمون‌های متفاوت با آزمون‌های فراهم شده برای سناریوی نخست را اجرا کند، برای نمونه، آزمون مدیریت تغییر را اجرا می‌کند، حتی اگر به تغییرات پیکربندی سامانه برنامه‌ریزی منابع بنگاه محدود شود. با این وجود، به‌علت تفاوت در سطح تکامل فناوری اطلاعات، میزان همپوشانی میان فضای فناوری اطلاعات و فضای مالی در سناریوی دوم، بیشتر خواهد بود.

اگر هدف حسابرسی در هر دو سناریو، استمرار کسب‌وکار باشد، از اینرو، به‌علت تفاوت در سطح تکامل فناوری اطلاعات، درمورد نخست، دامنه یا گستره آنچه حسابرس فناوری اطلاعات انجام خواهد داد، به‌طور کلی، به‌گونه‌ای درخور توجه، از مورد دوم (شرکت کوکاکولا) کوچکتر است.

سناریوی سومی هم وجود دارد که تفاوت در آن چشمگیر است. فرض شود مشتری، شرکتی کوچک با درآمد ۲ میلیون دلاری، دارای یک سرور و ۱۵ ایستگاه کاری است و تنها یک نرم‌افزار تجاری را به‌کار گرفته باشد. حسابرس فناوری اطلاعات با توجه به لزوم استمرار کسب‌وکار، چه کاری انجام خواهد داد؟ به‌گونه‌ای اطمینان‌بخش، آزمون (بازاجرای) داده‌های پشتیبان، به‌علت سطح پایین تکامل فناوری اطلاعات، نامربوط است. بنابراین در این مورد، حسابرس فناوری اطلاعات می‌تواند به پرس‌وجو از کارکنان کلیدی پیرامون نسخه‌های پشتیبان داده‌ها و این موارد بپردازد، امکان دارد تاییدیه مستقل از نسخه‌های پشتیبان داده‌ها، مبنی‌بر اینکه پشتیبان‌گیری اطلاعات به‌طور مرتب انجام می‌شود و در مکانی بیرون سایت به‌گونه‌ای ایمن ذخیره (انبارش) می‌شود (مشاهده یا پرس‌وجو). این دامنه از روش‌ها با سطح ریسک (ریسک تحریف بااهمیت) مرتبط با فناوری اطلاعات و این واحد تجاری انطباق دارد، به این معنی که بر پایه حسابرسی مبتنی‌بر ریسک و ارزیابی

> در حسابرسی مبتنی‌بر ریسک، به حسابرس فناوری اطلاعاتی نیاز است که سطحی مناسب از (دربرگیری) فضای فرعی در برنامه حسابرسی مالی را درنظر بگیرد تا بتواند به‌سوی کاهش در آن میزانی حرکت کند که مربوط به‌شمار آید

از ریسک، سطح ریسک مرتبط با استمرار کسب‌وکار، پایین است، بنابراین سطح آزمون مورد اجرا باید پایین باشد. در مورد شرکت کوکاکولا، اگر سامانه برنامه‌ریزی منابع بنگاه دچار نارسایی شود، در آن هنگام، فناوری اطلاعات، ریسک بااهمیت برای گزارش‌های مالی پدید می‌آورد. بنابراین، سطح ارزیابی ریسک مبتنی‌بر فناوری اطلاعات (ریسک تحریف‌های بااهمیت) و تکامل فناوری اطلاعات بسیار بزرگتر از مشتری کوچک است که در این مورد، گسترش مجموعه‌ای از روش‌های بسیار پیچیده‌تر، مناسب است (برای نمونه، هرچه ریسک تحریف‌های بااهمیت بالا باشد، به آزمون‌های سطح بالا نیاز است).

نتیجه‌گیری

هنگامی که حسابرسان فناوری اطلاعات در نقش حسابرسی مالی به‌کار گرفته می‌شوند، آنان باید دقت کنند تا دامنه مناسب از حسابرسی فناوری اطلاعات را گسترش دهند. این دامنه از موارد زیر تاثیر می‌پذیرد:

۱- درجه همپوشانی میان فضای گزارشگری مالی و فضای فناوری اطلاعات،

۲- درجه پیچیدگی فناوری اطلاعات که بر میزان همپوشانی تاثیر می‌گذارد، و

۳- همپوشانی ریسک تحریف بااهمیت و فضای فناوری اطلاعات.

از یک سو، پیامدهای این کار، تصمیم‌های معقولانه‌ای است که با پیروی از استانداردهای حسابرسی ناسازگاری دارد. در واقع، کار وظیفه‌شناسانه این است که پیرامون کاربست اصول حسابرسی مبتنی‌بر ریسک برای مشتری موجود، اندیشه کرد. به این معنی که، ارزیابی مناسب از سطح ریسک، موجب ایجاد تحرک در ماهیت، گستره و زمانبندی روش‌های حسابرسی بعدی می‌شود (به ویژه، آزمون‌های فناوری اطلاعات کنترل‌ها) و مهم‌تر، به تشخیص این مورد نیز کمک می‌کند که کدامیک حتی وجود دارند. ارزیابی مناسب از ریسک، نه تنها حسابرسی را به‌سوی اثربخشی بیشتر هدایت می‌کند (ریسک‌های بالا، آزمون‌های بالا می‌طلبد)، بلکه می‌تواند به‌سوی حسابرسی کارایی نیز، هدایت کند. دامنه بخش حسابرسی فناوری اطلاعات از حسابرسی مالی، به تنهایی بزرگتر از آنچه که نیاز است و به‌گونه‌ای ناخواسته، گسترده می‌باشد.

منبع:

- Singleton, Tommie W., What Every IT Auditor Should Know About Scoping an IT Audit, ISACA Journal, Vol. 4, 2009.

پی‌نوشت‌ها:

1. IT Portfolio
2. Sarbanes-Oxley (SOX) Act
3. Cyber Forensics
4. US Federal Bureau of Investigation (FBI)
5. Office of Inspector General (OIG)
6. Chief Information Officer (CIO)
7. Best Practices
8. Benchmarks
9. Systems Development Life Cycle (SDLC)
10. Information Technology General Controls (ITGC)
11. Operating System (O/S)
12. Virtual Machines
13. Control Objective for Information and Related Technology (COBIT)
14. Information Systems Audit and Control Association (ISACA)
15. Risk-Based Audit (RBA)
16. Overlap
17. Venn
18. Risk of Material Misstatement (RMM)
19. the American Institute of Certified Public Accountants (AICPA)
20. Control Risk (CR)
21. Inherent Risk (IR)
22. Gateway
23. Firewalls
24. Sophistication

۲۵. بیانیه استانداردهای حسابرسی (SAS) شماره ۹۴ «تاثیر فناوری اطلاعات بر ملاحظات حسابرسان پیرامون کنترل‌های داخلی در حسابرسی صورت‌های مالی»، جایگزین شده با استانداردهای حسابرسی مبتنی بر ریسک، چنین تمایزی را درباره پیچیدگی فناوری اطلاعات قایل شده است و بیان می‌دارد که اندازه واحد تجاری اهمیت ندارد، بلکه سطح تکامل فناوری اطلاعات آن دارای اهمیت است.

26. Microsoft Dynamics
27. Enterprise Resource Planning (ERP)

* کارشناس ارشد فناوری اطلاعات