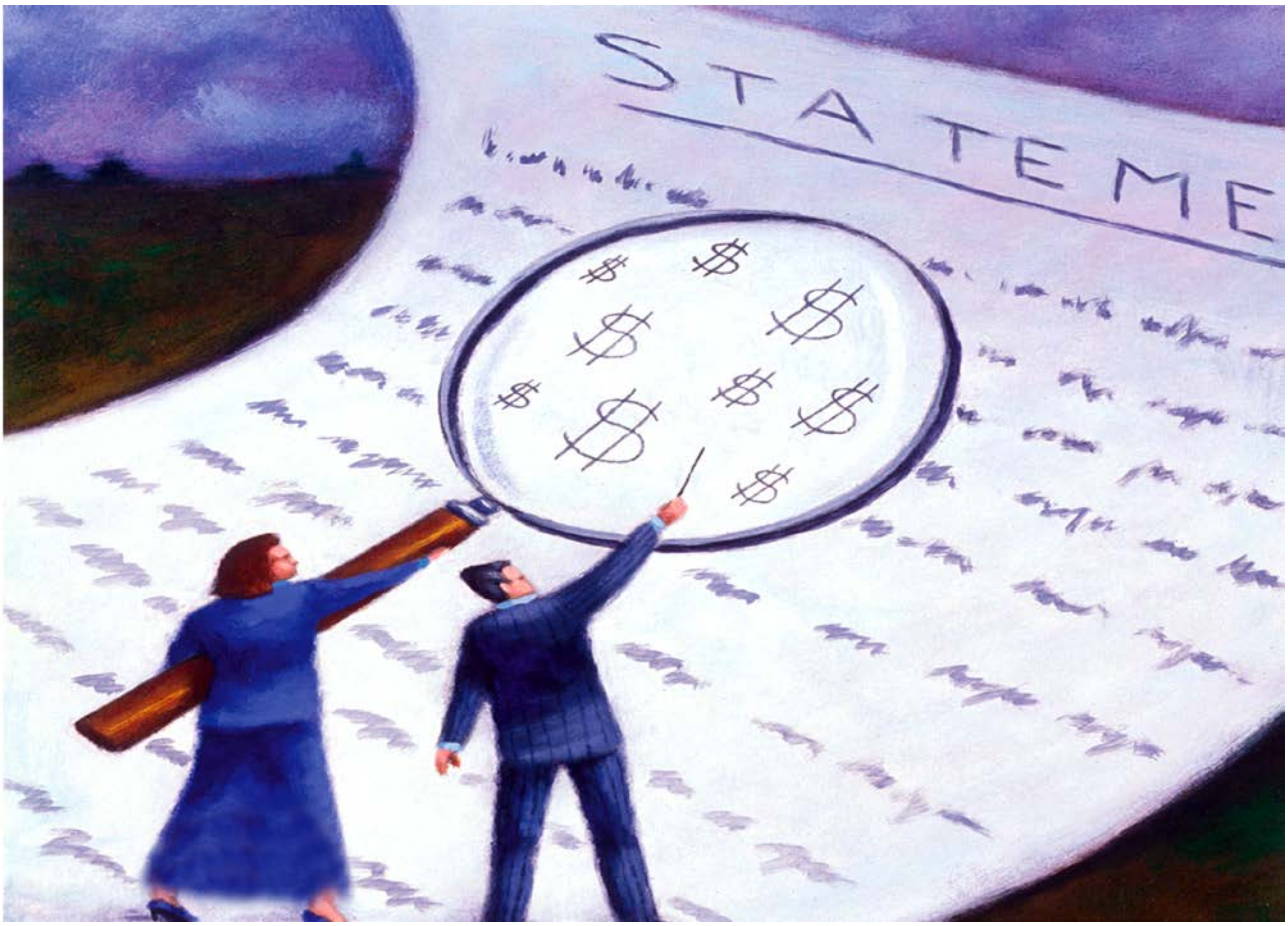
حسابرسی برنامه‌های کاربردی



ترجمه و تالیف: ابراهیم ابراهیمی، و
مریم اشرفی

مقدمه

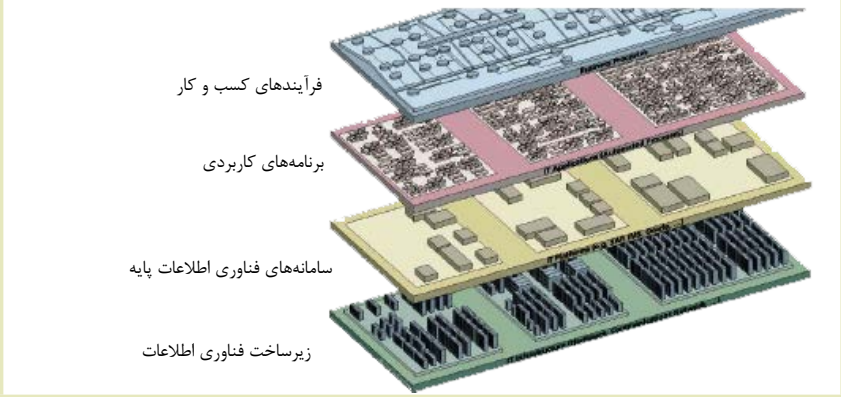
برنامه‌ی کاربردی یک برنامه‌ی رایانه‌ای است که برای انجام کارکردی معین مانند انبار، حسابداری حقوق و دستمزد، تجزیه و تحلیل، واژه‌پردازی، یا صفحه‌گسترده طراحی می‌شوند. برنامه‌های کاربردی در واقع تسهیل‌گر فرایندهای کسب‌وکار از راه فناوری اطلاعات هستند. به عبارتی، برنامه‌های کاربردی فرایندهای خودکارشده‌ای هستند که بخشی از یک یا چند فرایند کلی کسب‌وکار هستند. نمایه‌ی ۱ به‌خوبی جایگاه برنامه‌های کاربردی را در ساختار فرایندی کسب‌وکار نشان می‌دهد.

حسابرسی برنامه‌های کاربردی[1] نوع خاصی از حسابرسی در شرکت‌های متوسط و بزرگ است. این نوع حسابرسی، در واقع حسابرسی خاص یک برنامه‌ی کاربردی است، به ویژه، وقتی برنامه‌های کاربردی درون شرکت ایجاد شده باشند. مثلا، حسابرسی یک صفحه‌گسترده‌ی اکسل با کلان‌دستورهای تعبیه‌شده‌ی مورد استفاده برای تجزیه و تحلیل داده‌ها و ایجاد گزارش‌ها می‌تواند نمونه‌ای از یک حسابرسی برنامه‌ی کاربردی باشد. حسابرسی برنامه‌ی کاربردی همچنین می‌تواند به فرایند کسب‌وکاری مربوط باشد که زیاد به سامانه‌های فناوری اطلاعات مختلف تکیه می‌کند. یک نمونه، فرایند حقوق و دستمزد شرکت است که می‌تواند بین چندین سرور مختلف، دادگان، سامانه‌های عملیاتی (سامانه‌های عامل) برنامه‌های کاربردی و غیره احاطه شده باشد.

در این نوع حسابرسی، حسابرس به دنبال اطمینان از آن است که برنامه‌ی کاربردی درجه‌ی کنترل کافی بر داده‌های مورد پردازش به‌دست می‌دهد. سطح کنترل مورد انتشار برای یک برنامه‌ی کاربردی خاص وابسته به میزان ریسک موجود در پردازش نادرست یا غیرمجاز آن داده‌ها است. به هر روی، در حسابرسی برنامه‌ی کاربردی حداقل باید از وجود کنترل‌هایی بر موارد زیر اطمینان داد:

- **اداره**- اداره‌ی برنامه‌ی کاربردی احتمالا مهم‌ترین حوزه‌ی مورد بررسی در حسابرسی برنامه‌ی کاربردی است. زیرا، این حوزه بر مالکیت کلی و حساب‌دهی برنامه‌ی کسب‌وکار تمرکز دارد. بدون کنترل کافی بر اداره‌ی یک برنامه‌ی کاربردی حوزه‌های دیگر احتمالا نمی‌توانند اطمینان دهند که کنترل‌ها بجا هستند و ریسک‌ها را کاهش می‌دهند. در واقع، حسابرس باید اطمینان یابد که مسئولیت‌ها و نقش‌ها به طور واضح تعریف و مستند شده‌اند. به عبارت دیگر، هدف شناخت ساختار سازمانی برنامه‌ی کاربردی است، به گونه‌ای که ملاحظات مربوط به تفکیک وظایف، مالکان و مسئولان، پشتیبان و خدمات‌رسان و مسئولیت‌ها به‌خوبی تعریف شده باشد.
- **ورودی، پردازش، خروجی**- در این حوزه، حسابرس به دنبال شواهدی از روش‌های تدارک داده‌ها، فرایندهای مغایرت‌گیری، الزامات اجرا و غیره است. در این مورد در ادامه بیشتر توضیح داده خواهد شد. ولی، این جا به همین

نمایه‌ی ۱
جایگاه برنامه‌های کاربردی در ساختار فرایندی کسب‌وکار



بسنده می‌شود که حسابرس باید خود را برای بررسی فرایندهای کسب‌وکار پیرامون ایجاد تراکنش‌هایی که وارد سامانه خواهند شد، آماده کند؛ نمونه‌ای از مستندات منبعی را درخواست کند؛ و نسخه‌هایی از گزارش‌های خروجی برنامه‌ی کاربردی را دریافت کند.

- **امنیت منطقی**- حسابرسی برنامه‌ی کاربردی معمولا مستلزم ارزیابی عمیق امنیت برنامه‌ی کاربردی است. این بررسی در بالاترین بررسی امنیت منطقی اجراشده به عنوان بخشی از بررسی زیرساخت‌ها در سطح سامانه‌ها انجام می‌شود.
- **طرح بازیابی بلا**- حسابرسان به طور خاص از ضرورت کفایت یک طرح بازیابی بلا که اطمینان کافی از بازیابی برنامه‌ی کاربردی در زمان منطقی پس از وقوع یک بلای طبیعی یا حادثه‌ی غیرمنتظره فراهم سازند، آگاه هستند. در این زمینه، حسابرس رهنمودهای پشتیبان‌گیری و مستندات فرایندهای آن را درخواست خواهد کرد.
- **مدیریت تغییر**- همه‌ی تغییرات در برنامه‌ی کاربردی باید در فرایند رسمی و استانداردشده‌ای انجام شود. حسابرس باید اطمینان یابد که این فرایند مستند و دنبال می‌شود. سنگ‌بنای یک سامانه‌ی مدیریت تغییر این است که همه‌ی تغییرات مستند شود، اعم از این که مشکلات را رفع کند یا تقویت بخشد.
- **پشتیبانی کاربر**- حسابرس باید اطمینان یابد مستندسازی کاربر درباره‌ی برنامه‌ی کاربردی، به شکل راهنماها و دستورالعمل‌های کاربردی، کمک برخط و غیره، آماده و دسترس کاربر و به‌روز هستند.

در هر حال، برای این که بتوان یک حسابرسی برنامه‌ی کاربردی موفق داشت، باید یک چارچوب کلی را دنبال کرد. این چارچوب در ادامه مورد بحث قرار می‌گیرد.

چارچوب حسابرسی برنامه‌ی کاربردی

چند اصل بنیادی برای حسابرسی برنامه‌های کاربردی وجود دارد که حسابرسان فناوری اطلاعات باید آنها را بشناسند و درک کنند. این اصول در قالب یک چارچوب فرایندمحور بیان می‌شوند. چارچوب فرآیندمحور شامل مراحلی مشابه زیر است:

- طرح‌ریزی حسابرسی
- تعیین اهداف حسابرسی
- نگاشت (نقشه‌برداری)[۲] سامانه‌ها و گردش داده‌ها
- شناسایی کنترل‌های کلیدی
- شناخت کارورسازی (عاملیت)[۳] برنامه‌ی کاربردی
- اجرای آزمون‌های کاربردپذیر
- دوری کردن/در نظر گرفتن پیچیدگی‌ها
- در بر گرفتن گزاره‌ها (ادعاها)ی مالی
- توجه به ابزارهای سودمند
- تکمیل گزارش

بعضی از مراحل مانند نگاشت سامانه‌ها و گردش داده‌ها فراگیر هستند. از آن جا که نگاشت باید در ابتدای کار حسابرسی انجام شود، تقریبا نقش مهمی را در دیگر مراحل ایفا می‌کند. دیگر مراحل مانند ادعاهای مالی ممکن است کاربرد داشته باشند و حتی ممکن است کاربرد نداشته باشند. با این وجود، چارچوب پیش‌گفته بدنه‌ی منصفانه‌ای از مراحلی است که برای انجام اثربخش حسابرسی برنامه‌های کاربردی باید انجام شوند. در ادامه این مراحل تشریح می‌شوند.

(۱) طرح ریزی حسابرسی

طرح‌ریزی حسابرسی شامل ملاحظه‌ی همه‌ی عوامل مربوطی است که هدف حسابرسی را شکل می‌دهند. این ملاحظه، برای طرح‌ریزی مناسب حسابرسی لازم است.

ملاحظه‌ی هدف

یکی از محرک‌های کلیدی حسابرسی برنامه‌های کاربردی، در کل فرایند، شرایط یا موقعیت‌هایی است که توجیه‌کننده‌ی حسابرسی بوده‌اند. به این معنی که چه عاملی نیاز به حسابرسی را ایجاب می‌کند؟ آیا این نیاز یک طرح حسابرسی منظم است؟ یا تنها یک حسابرسی موردی است؟ این نیاز معمولا مستقیما به هدف اولیه‌ی حسابرسی مرتبط است. برای مثال، اگر مدیریت بخواهد اطمینان یابد که یک برنامه‌ی کاربردی همان طور که طراحی شده است کار می‌کند، این خود عاملی است که اهداف و طرح حسابرسی را جهت‌دهی خواهد کرد.

ملاحظه‌ی ریسک

دومین عامل و محرک کلیدی، در نظر گرفتن ریسک مربوط به یک حسابرسی خاص است؛ با دانستن این که هدف آن حسابرسی قبلا تعیین شده است. حسابرس فناوری اطلاعات، یا تیم حسابرسی، نیازمند شناسایی ریسک مربوط به برنامه‌ی کاربردی و داده‌های مربوط به آن، منابع، زیرساخت، و سامانه‌های مربوط به آن است. در ادامه‌ی مثال قبلی، سناریوهای احتمالی ریسک شامل عدم کارورسازی (به این معنی که نیازهای اطلاعاتی واقعا محقق نمی‌شود) خطاها و ایرادها، ناتوانی در انسجام/تعامل با دیگر برنامه‌های کاربردی یا سامانه‌ها، خطاهای داده‌ای، و دیگر ریسک‌های مشابه است. مسلما وقتی سناریوهای ریسک به درستی مشخص شوند، حسابرس فناوری اطلاعات باید اثرات آن را روی اهداف حسابرسی، طرح حسابرسی، دامنه‌ی حسابرسی و روش‌های حسابرسی ارزیابی کند. برای نمونه، اگر نبود کارورسازی یک ریسک است، حسابرس فناوری اطلاعات باید نیازهای اطلاعاتی اولیه را رسیدگی کند، آزمون‌ها را بازبینی کند، سند پذیرش کاربر (در صورت وجود) را بازبینی کند، برنامه‌ی کاربردی را آزمون کند و دیگر روش‌های مشابه را اجرا کند.

ملاحظه‌ی محیط کنترلی

معمولا طرح حسابرسی باید محیط کنترلی احاطه‌کننده‌ی برنامه‌ی کاربردی را در راستای هدف حسابرسی در نظر بگیرد. اگر هدف اولیه‌ی حسابرسی، حسابرسی کارورسازی مناسب است، کنترل‌ها ممکن است از نوع کنترل‌های توسعه‌ی برنامه‌ی کاربردی یا کنترل‌های چرخه‌ی عمر توسعه‌ی سامانه‌ها[۴] باشند. به طور خاص، کنترل‌ها برای آزمون برنامه‌ی کاربردی مهم هستند

ملاحظه‌ی پیش/پس اجرا

گاهی حسابرسی برنامه‌ی کاربردی مستلزم یک برنامه‌ی کاربردی پیشااجرایی است. ولی، به احتمال زیاد، این یک موقعیت پسااجرایی خواهد بود. پیشاحسابرسی‌ها[۵] مستلزم اهداف خاص، و دامنه و روش‌های معینی هستند که خاص آن برنامه‌ی کاربردی و هدف هستند. پساحسابرسی‌ها[۶] معمولا مجموعه‌ای از اهداف کلی را دنبال می‌کنند.

ملاحظه‌ی هدف

یک ملاحظه‌ی خیلی مهم در طرح‌ریزی، ایجاد آستانه‌ها و محدودیت‌های دامنه است. به این معنی که فناوری‌های مربوط

و کنترل‌های مرتبط با حسابرسی برنامه‌های کاربردی مشخص شوند، مانند:

- تعامل با دیگر برنامه‌های کاربردی
- سامانه‌های منبعی
- سامانه‌های مقصد/هدف
- زیرساخت‌ها یا اجزای مربوط به آنها
- دادگان
- منطقه‌ی عملیات/قابلیت آزمون

ملاحظه‌ی شایستگی‌ها

همانند همه‌ی حسابرسی‌ها، یکی از سرپرستان یا مدیران تیم حسابرسی باید صلاحیت‌ها و شایستگی‌های تیم را با توجه به احتیاج‌های حسابرسی ارزیابی کند. به طور مثال، اگر رابط دربرگیرنده‌ی اوراکل باشد، به یک متخصص در زمینه‌ی اوراکل برای حسابرسی درست برنامه‌ی کاربردی نیاز است.

(۲) تعیین اهداف حسابرسی

اهداف تا حدودی وابسته به ملاحظه‌ی پیشا/پسا اجرایی است. همان طور که قبلا گفته شد، اهداف گرایش به اختصاصی بودن برای برنامه‌های کاربردی پیشااجرایی دارند. همین موضوع برای اهداف معین صادق است. در دیگر موارد، هدف به یکی از مواردی که به حسابرسی‌ها مربوط است، گرایش دارد:

- کارایی (مربوط به هزینه‌های توسعه، عملکرد عملیاتی و غیره)
- اثربخشی (مربوط به تحقق نیازهای اطلاعاتی/کارورسازی، هدف تایید اولیه، یکپارچگی با دیگر فناوری‌های اطلاعاتی، عملکرد عملیاتی و غیره)
- رعایت (قوانین و ضوابط، قراردادی و غیره)
- هشدارها (اگر هشدارها با برنامه‌ی کاربردی درگیر است)
- ملاحظات گزارشگری مالی

(۳) نگاشت سامانه‌ها و گردش داده‌ها

نگاشت (نقشه‌برداری) یکی از موثرترین ابزارهایی است که حسابرس فناوری اطلاعات در هر کار حسابرسی فناوری اطلاعات دارد. در حسابرسی برنامه‌های کاربردی، مهم است که دامنه‌ی دیگر فناوری‌های اطلاعاتی را که بر برنامه‌ی کاربردی مورد حسابرسی اثر می‌گذارند یا تحت تاثیر آن قرار می‌گیرند، به درستی تعیین کرد. کارشناسان بر این باور هستند که نگاشت می‌تواند به حسابرس فناوری اطلاعات در کسب یک شناخت کلی از فناوری‌های مربوط، فرآیندها، کنترل‌های مربوط و چگونگی انسجام آنها به یکدیگر کمک کند. همچنین، به حسابرس فناوری اطلاعات قدرت می‌دهد تا مراحل این چارچوب را از طرح‌ریزی تا گزارشگری به بهترین شکل انجام دهد، به این معنی که نگاشت اثر فراگیری بر کیفیت حسابرسی فناوری اطلاعات دارد.

مواردی (در بین دیگر موارد) که باید در نگاشت درست

نمایه‌ی ۲

مثال نگاشت (نقشه) با استفاده از کاربرگ

بخش اول

فناوری اطلاعات	شرح	O/S	سامانه‌ی مدیریت دادگان(DBMS)	سرور دادگان	محل داده‌ها
برنامه‌ی کاربردی ABC	میان‌افزارها طراحی‌شده برای.....	م.ن	م.ن	XYZ	بیرمنگام
برنامه‌ی کاربردی DEF	مدیریت ارتباط با مشتری، هدف.....	Z/OS	DB2	پردازنده‌ی مرکزی Z	شهر نشویل

بخش دوم

توسعه‌یافته	نگهداری	مالک	مسئول دسترسی	کنترل تغییرات	یادداشت‌ها
داخل شرکت	داخل شرکت	سو	مدیریت فعال...	کنترل‌ها شامل...	
فروشنده	فروشنده،	جان	مسئول امنیت....	فروشنده.....	

نمایه‌ی ۳

مستندسازی و نگاشت (نقشه‌برداری) ریسک‌ها

بخش ۱

ردیف	ریسک	حوزه‌ی ریسک	هدف	رفرنس W/p	روش‌ها
۱	داده‌های نامعتبر، نادرست یا ناقص ممکن است موجب بروز خطاهایی در گزارش‌ها یا حسابداری شوند.	درستی داده‌ها	ارزیابی بررسی‌های درستی داده‌ها، و کنترل‌های بین ورودی‌ها و خروجی ها	C.O۱.۱	
۲	تغییرات غیر هدفمند یا بدون مجوز در میان‌افزار ممکن است باعث ایجاد خطا در گزارش‌ها یا حسابداری شود.	مدیریت تغییر	ارزیابی تغییرات در برنامه‌های کاربردی از لحاظ تصویب، آزمون‌ها و تفکیک وظایف	C.O.۱.۲	
۳	دسترسی غیرمجاز ممکن است موجب تغییرات غیرمجاز در میان‌افزار یا داده‌های هدف شود که در نتیجه باعث خطا در گزارش‌ها یا حسابداری می‌شوند.	امنیت	ارزیابی کنترل‌های دسترسی منطقی به برنامه‌ی کاربردی و فایل آن	C.O.۱.۳	
۴	پردازش نامعتبر، نادرست یا ناقص ممکن است موجب خطاهایی در گزارش‌ها یا حسابداری شود	عملیات	ارزیابی پردازش و مستندسازی برای کنترل‌های مناسب روی توسعه و پشتیبانی و شناسایی و رفع خطا	C.O.۱.۴	

بخش ۲

مرجع	روزهای حسابرسی	درصد انجام کار	روزهای باقی مانده تا تکمیل	دامنه‌ی سامانه‌ها	توضیحات
۱	۰,۵	%۱۰۰	۰	میان‌افزار، روش‌های ذخیره، دیدگاه‌ها، مدیریت ارتباط با مشتری، دادگان ۲(DB۲)	
۲	۱,۵	%۳۳	۱	میان‌افزار	
۳	۱,۰	%۰	۱	راهنمای فعال، میان‌افزار	
۴	۲,۰	%۰	۲	**ورودی**: فایل منبع **پردازش**: میان‌افزار **خروجی**: فایل هدف/DB۲، گزارش خطاها	

بخش۳

ردیف	ریسک ذاتی	ریسک کنترل	ریسک ارزیابی‌شده	توضیحات
۱	بالا	متوسط	متوسط - بالا	تا امروز، واقعیات رخ داده .....
۲	متوسط	پایین	پایین	
۳	بالا	متوسط	متوسط – بالا	
۴	متوسط	پایین	پایین - متوسط	

برنامه‌ی کاربردی در نظر گرفته شود، عبارت‌اند از:

- اجزای فناوری اطلاعات مرتبط (شرح)
- صاحبان کسب‌وکار یا خطوط کسب‌وکار
- خط‌مشی‌ها و روش‌های مدیریت تغییر نقش و اثر فروشندگان
- فرایندهای کسب‌وکار
- کنترل‌ها
- اداره‌ی دسترسی و امنیت

این عوامل می‌توانند حسابرس فناوری اطلاعات را در ایجاد نقشه، تعیین آن چه باید در نقشه باشد یا مشخص کردن این که چه ستون‌هایی باید در کاربرگی که نقشه را نمایش می‌دهد وجود داشته باشد، راهنمایی می‌کند. نمایه‌ی ۲ روشی برای نگاشت (نقشه‌برداری) حسابرسی برنامه‌ی کاربردی را نشان می‌دهد.

مستندسازی و نگاشت ریسک ممکن است شامل اقلامی مانند ریسک، حوزه‌ی ریسک، هدف، ماخذ، روش‌ها، روزهای حسابرسی، درصد کار انجام‌شده، روزهای باقی‌مانده تا تکمیل کار، دامنه‌ی سامانه‌ها و یادداشت‌ها باشد. نمایه‌ی ۳ کاربرگی را نشان می‌دهد که ممکن است در نگاشت ریسک مفید باشد، و نشان می‌دهد که چگونه این نقشه‌ی نگاشته‌شده، می‌تواند در سرتاسر کار حسابرسی سودمند باشد و ممکن است در اداره‌ی کار حسابرسی کمک‌رسان باشد.

حسابرسان فناوری اطلاعات نیازمند نگاشت فرایند و گردش داده‌ها با استفاده از ابزارهای متداول از قبیل نمودارهای گردش داده، فلوچارت سامانه‌ها یا زبان مدل‌سازی همه‌منظوره[۷] هستند. گاهی ممکن است استفاده از یک نمودار نامتداول برای به تصویر کشیدن فرایندها و گردش داده‌ها بهتر باشد. برای مثال، ماتریس نمایه‌ی ۴ ممکن است مدل بهتری باشد زیرا زمان/ تحویل را علاوه بر سامانه‌ها، فرایندها و گردش داده‌ها نشان می‌دهد.

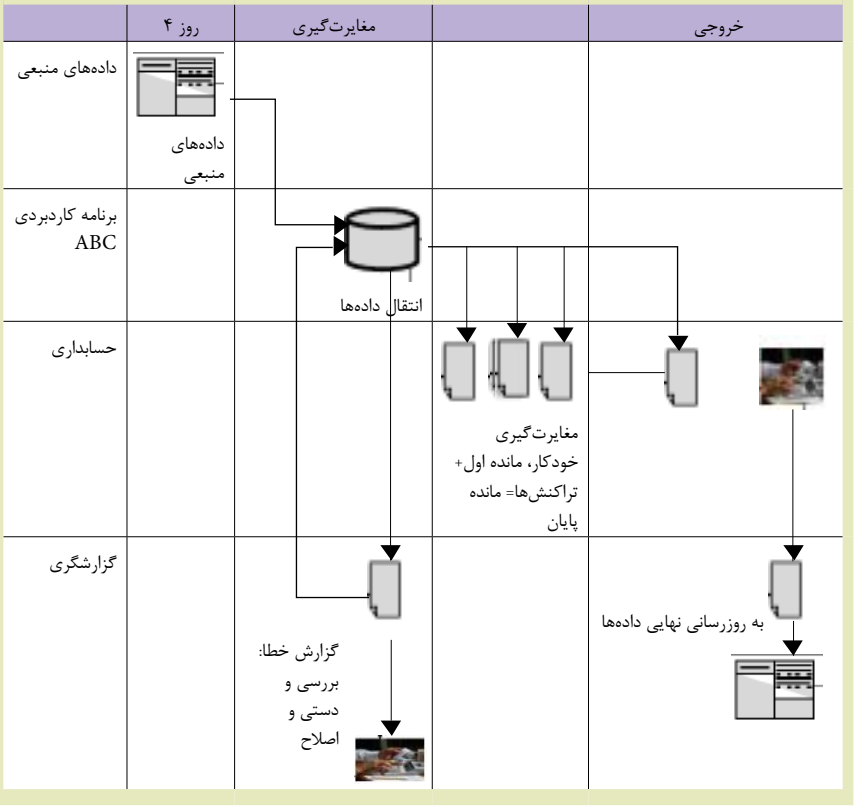
ترسیمه‌ی خاصی که در نمایه‌ی ۴ نمایش داده شده است، کنترل‌ها را به روشی واضح و قابل فهم شرح داده است. برای مثال، مغایرت‌گیری خودکار، سامانه‌ی کنترل خطاها (وابسته به فناوری اطلاعات)، و بررسی‌های دستی داده‌های CRM (مدیریت ارتباط با مشتری) قبل از این که داده‌های هدف به عنوان یک کنترل در گردش داده و فرایندها بارگذاری شوند.

این چارچوب فرایند/ گردش داده ممکن است زمانی اثربخش‌تر باشد که با استفاده از مدل سامانه‌ای در مقابل ابعاد فرایندی و چارچوب زمانی ارائه شود. ورودی‌ها شامل داده‌های منبعی، مانند داده‌های منبعی برای استفاده‌ی برنامه‌ی کاربردی میان‌افزار است. آنها همچنین شامل داده‌های میانی نیز هستند. منابع شامل دادگان داخلی و خدمات‌رسان‌های خارجی داده‌ها است.

بخش پردازش شامل کارکرد پردازش برنامه‌ی کاربردی است. (نمایه‌ی ۴ را ببینید که دربرگیرنده‌ی مغایرت‌گیری خودکار و جریان عادی کشف/اصلاح خطا است). همچنین، شامل مدارک هر فرایندی است که برای کارکردهای پردازش

نمایه‌ی ۴

نگاشت(نقشه برداری) فرایندها و گردش داده‌ها



ایجاده شده است. بعضی از فرایندها شبیه به فرایندهای مربوط به انبارش داده‌ها، از قبیل ETL (استخراج، انتقال و بارگذاری) هستند که اساسا توصیف می‌کنند داده‌های فرایند از منابع مختلف جریان می‌یابد تا در انباره‌ی داده‌ها جای گیرند. برای مثال، برنامه‌ی کاربردی ABC در نمایه‌ی ۴ نسبتا با ETL سازگار است. منطق پردازش در برنامه‌های کاربردی دارای توجه خاص است، زیرا جز اصلی درستی و اتکاپذیری داده‌ها است.

خروجی‌ها شامل گزارش‌ها، اطلاعات دیداری، و دیگر مدارک چاپی است. خروجی‌ها نیز نیازمند ارزش‌یابی ابزارها و الگوهای مورد استفاده برای ایجاد گزارش‌ها و تصاویر هستند.

(۴) شناسایی کنترل‌های کلیدی

وقتی کنترل‌های مربوط ارزیابی می‌شوند، ممکن است حسابرس فناوری اطلاعات بخواهد بین کنترل‌های سفارشی و کنترل‌هایی که در نرم‌افزارهای تجاری آماده‌ی مصرف (COTS)[۸] وجود دارند، تمایز قائل شود. برای کنترل‌های سفارشی ساخته‌شده، پرس‌وجو یک راه‌کار خوب برای شروع ارزیابی است. یکی از پرسش‌های کلیدی این است که از مدیریت درباره‌ی ماهیت خاص کنترل‌هایی که به صورت تخصصی وارد فرایند توسعه‌ی برنامه‌ی کاربردی شده‌اند، پرسیده شود. به این معنی که چه کسانی یا چه گروهی تخصص این را دارند که از کفایت کنترل‌های تعبیه‌شده در برنامه‌های کاربردی جدید اطمینان حاصل کنند؟ چگونه می‌توان به آن هدف رسید؟ و در آخر، حسابرس فناوری اطلاعات باید اطمینان یابد که کنترل‌ها به‌درستی مستند و آزمون شده‌اند.

برای نرم‌افزارهای تجاری آماده‌ی مصرف، حسابرس فناوری اطلاعات احتمالا کار خود را با آزمون شناخت سامانه آغاز می‌کند تا مشخص کند چه کنترل‌هایی واقعا در برنامه‌ی کاربردی به کار گرفته شده‌اند و چگونه کار می‌کنند. آزمون شناخت سامانه شامل تراکنش‌ها یا فرایندهای پشت سر هم گام به گام، همراه با شخص مسئول ورود داده‌ها است که توضیح می‌دهد چه کاری و چرا انجام شود. چنین فرایندی باید به حسابرس فناوری اطلاعات این توان را بدهد که درک کلی از کنترل‌های برنامه‌های کاربردی، کفایت کنترل‌ها و ماهیت آن‌ها (مثل اثربخشی) به‌دست آورد. این آزمون شناخت سامانه به‌ویژه در مواقعی ضروری است که برای نخستین‌بار از برنامه‌ی کاربردی استفاده می‌شود. همچنین، در نرم‌افزارهای تجاری آماده‌ی مصرف حسابرس فناوری اطلاعات باید مبنایی از کنترل‌ها ایجاد کند- باید آزمون‌هایی برای شناخت اتکاپذیری و اثربخشی انجام شود.

برای نرم‌افزارهای تجاری آماده‌ی مصرف، حسابرس فناوری اطلاعات باید مسئولیت فروشندگان را نیز مشخص کند. به خاطر وجود این هدف است که نمایه‌ی ۲، اطلاعاتی درباره‌ی فروشنده و نوع نگهداری از برنامه‌ی کاربردی دارد. وقتی مشکلی

در برنامه‌ی کاربردی رخ می‌دهد، مدیر نیاز دارد از این که برای حل مشکل دقیقا به چه کسی تکیه کند، اطمینان یابد. واضح است که شیوه‌های مدیریت فروشنده اعمال می‌شود.

انواع کنترل‌ها می‌تواند با استفاده از مدل‌های سامانه‌ای معمول یعنی ورودی، پردازش و خروجی ارزیابی شوند. کنترل‌های ورودی شامل این موارد می‌شود:

- امنیت‌دسترسی
- تفکیک منطقی وظایف
- معتبرسازی داده
- درستی داده‌ها
- کدینگ
- اصلاح اشتباه‌های ورودی
- کنترل‌های دسته‌ای (در صورت کاربرد)
- کنترل‌های معمول پردازش شامل موارد زیر هستند:
- سطح اتوماسیون (برای مثال تماما خودکار، وابسته به فناوی اطلاعات، تماما دستی)
- جدول زمان‌بندی کار یا سفارش (برای پردازش سفارش)
- پایش زمان‌بندی سفارش
- محاسبات خودکار
- مغایرت‌گیری خودکار
- اطلاعیه‌های خودکار
- کنترل‌های معمول خروجی عبارت‌اند از:
- مغایرت‌گیری‌ها
- بازبینی‌ها
- تاییدیه‌ها
- کشف خطاها/گزارش‌ها یا فهرست خطاها
- کنترل روی گزارش‌های فیزیکی (کنترل جانبی)

(۵) شناخت کارورسازی برنامه‌های کاربردی

به‌طور معمول کارورسازی حسابرسی هدف مهم حسابرسی است. روش‌ها مستلزم تایید کارورسازی عملیاتی است که باید در نیازهای اطلاعاتی در فرایند توسعه‌ی برنامه‌ی کاربردی توصیف شوند. حسابرس فناوری اطلاعات در کنار بازبینی مدرک تایید برای برنامه‌ی کاربردی، باید گزارش پذیرش کاربر نهایی را در صورت وجود، بازبینی کند. عدم وجود چنین گزارشی نشان‌دهنده‌ی ضعف در کفایت روش‌های کنترلی برای فرایند توسعه‌ی برنامه‌ی کاربردی است.

بعضی از اهداف معمول به هدف برنامه‌ی کاربردی مربوط است. به‌هنگام آزمون برنامه‌ی کاربردی باید سناریوهای مختلف برای آزمون مناسب برنامه‌ی کاربردی را مورد توجه قرار داد. اگر هدف برنامه‌ی کاربردی منجر به نتیجه‌ی دوگانه شود، آزمون یکی آن‌ها ممکن است کافی باشد (بله یا نه، تصویب یا عدم تصویب، و غیره). ولی اگر برای مثال برنامه‌ی کاربردی، به روزرسانی پردازش حقوق و دستمزد است، چندین سناریو وجود خواهد داشت که برای آزمون همه‌ی ترکیب‌های مختلف عواملی که وارد محاسبه‌ی مالیات‌های حقوق و دستمزد می‌شوند، در نظر گرفته شوند. ارزیابی کنترل‌های امنیت و دسترسی هم احتمالا به نتیجه‌ی مشابه می‌رسد.

بعضی ملاحظات خاص، شامل حداقل دو چیز می‌شوند که کاربر نهایی و مدیر کسب‌وکار تمایل دارند در مرحله‌ی جمع‌آوری نیازهای اطلاعاتی آنها را نادیده بگیرند: امنیت و دامنه‌ی مناسب داده‌های ضبط‌شده. سطح مناسب امنیت به طور واضح یک عامل موفقیت کلیدی در فرایند توسعه‌ی برنامه‌ی کاربردی است و بنابراین باید ارزیابی شود. معمولا کاربران و مدیران به طور کامل دامنه‌ی داده‌هایی را که باید در آغاز تراکنش‌ها و رویدادها بدانند، نمی‌دانند. این حقیقت به‌ویژه وقتی مهم است که شرکت طرح‌هایی برای به‌کارگیری ابزارهای همچون هوش کسب‌وکار یا تحلیل‌های کسب‌وکار دارد.

بسته به ملاحظه‌ی هدف، کنترل‌های عملیاتی ممکن است در دامنه قرار گیرند. مشابه این برای کنترل‌های گزارشگری مالی مصداق دارد.

استفاده از مدل سامانه‌ای به احتمال زیاد تجزیه و تحلیل و آزمون کارورسازی برنامه‌ی کاربردی را راحت‌تر و کامل‌تر می‌کند.

(۶) اجرای آزمون‌های کاربردپذیر

وقتی یک برنامه‌ی کاربردی به درستی انجام نمی‌شود، وقتی خطاهایی رخ می‌دهد، وقتی فرآیندهای تعبیه‌شده در برنامه‌ی کاربردی به درستی کار نمی‌کنند، مشکل معمولا می‌تواند با ردیابی رو به عقب به فاز آزمون مرحله‌ی نادرست پیدا شود. آزمون برنامه‌ی کاربردی، معمولا چیزی فراتر از صرفا یک آزمون است.

بهترین رویه برای آزمون، مستلزم چندین سطح آزمون است. نخست، برنامه‌ی کاربردی به تنهایی آزمون شود. معمولا این کار توسط برنامه‌نویس ارشد یا تحلیل‌گری انجام می‌شود که مسئولیت اصلی پروژه‌ی توسعه‌ی برنامه‌ی کاربردی را بر عهده دارد. سپس برنامه‌ی کاربردی برای انجام کنترل‌های کیفی به واحد فناوری اطلاعات ارسال می‌شود. به این معنی که برنامه‌ی کاربردی توسط متخصصان واحد فناوری اطلاعات آزمون می‌شود.

پس از آن، برنامه‌ی کاربردی توسط کاربران واقعی آزمون می‌شود. اغلب این کاربران نهایی به شیوه‌ی چرخشی همزمان با توسعه‌ی برنامه‌ی کاربردی، در کار درگیر هستند. اما حداقل یک یا چند کاربر نهایی باید برنامه‌ی کاربردی را همین که به طور کامل توسعه یافت، آزمون کنند تا کارورسازی، کامل بودن، صحت و کارایی آن را مشخص کنند. بعد از تکمیل، متداول است که کاربر نهایی گزارش پذیرش کاربر نهایی را امضا کند که در آن نتایج آزمون مستند می‌شود.

سپس، برنامه‌ی کاربردی همراه با سایر برنامه‌های کاربردی در همان ماژول، چرخه، یا طبقه‌ی تراکنش‌ها آزمون می‌شود. این کار اغلب مستلزم یک محیط قوی‌تر از آزمون اولیه‌ی برنامه‌ی کاربردی به تنهایی است. نقطه‌ی سکویی، یکی از بهترین راه‌ها برای انجام این آزمون است. در این نقطه یک شبیه‌ساز از زیر ساخت‌ها، برنامه‌های کاربردی، سامانه‌ها و دادگان ایجاد می‌شود.

ولی این پایان کار نیست. برنامه‌ی کاربردی باید در بافتار سامانه‌ی بنگاه، با همه‌ی انتقالات و ارتباط داده‌ها که در عملیات واقعی فناوری اطلاعات انجام می‌شوند، آزمون شود. این فرایند به طور خاص به یک منطقه‌ی سکویی نیاز دارد.

(۷) دوری کردن یا در نظر گرفتن پیچیدگی‌ها

پیچیدگی‌هایی وجود دارند که ذاتا ریسکی هستند. بنابراین، در طول حسابرسی باید به آنها توجه کرد. اول، برنامه‌های کاربردی خاص (سفارشی) ریسک ذاتی بالایی دارند. این واقعیت روی اهداف، برنامه‌ریزی، کنترل‌ها و مراحل ریسک اثر می‌گذارد.

اگر انباره‌ی داده درگیر کار هست، ریسک ذاتی نسبتا بالایی وجود خواهد داشت. تقریبا به طور کامل، وقتی یک انباره‌ی داده برای اولین بار پیاده‌سازی می‌شود، داده‌هایی که وارد انباره‌ی داده می‌شوند، به دلایلی مثل ناسازگاری در داده‌ها (فیلدهای یکسان با نام‌های متفاوت)، داده‌های ازقلم‌افتاده و داده‌ی بد (یعنی خطاها) ریسک بالایی دارند. بنابراین، وقتی داده‌ها از سامانه‌های پردازش تراکنش‌ها استخراج می‌شوند، باید در نگاشت (نقشه‌برداری) داده‌ها دقت لازم اعمال شود و از فرایند ETL(استخراج ، انتقال و بارگذاری) برای شناسایی و اصلاح نابهنجاری‌های داده که قبلا اشاره شد، استفاده شود.

برای انباره‌ی داده در حال اجرا، صاحبان داده‌ها برای مثال می‌توانند نام فیلدها را تغییر دهند، فیلدهایی را اضافه کنند و اگر کنترل‌های تغییرات موثر نباشند، داده‌ها نمی‌توانند با موفقیت وارد فرایند ETL بعدی شوند. بنابراین، کنترل‌های مدیریت تغییرات برای انباره‌ی داده‌ها خیلی مهم هستند. این نکته برای سایر کارکردهای مشابه هم صادق است.

باید بین دو نوع از ریسک مربوط به انباره‌ی داده تمیز قائل شد. نخست، در این جا درستی پردازش وجود دارد. این درستی درباره‌ی این است که آیا پردازش موفق بوده است یا نه. آیا برنامه‌ی کاربردی آن چه را که باید راجع به نقش پردازشی‌اش انجام می‌داد، انجام داده است؟ دوم، درستی داده یا کیفیت داده‌ای وجود دارد که اتکاپذیری و درستی داده‌هایی را که پردازش، منتقل و ثبت می‌شوند، در بر می‌گیرد. آیا اطلاعات وارد شده معتبر است؟ آیا داده‌های منبعی معتبر، صحیح و کامل هستند؟ آیا انتقال داده‌ها از منبع به مقصد به طور موثر و بدون خطایی کامل شده است؟

(۸) شمول ادعاهای مالی

وقتی گزارشگری مالی در دامنه‌ی کار قرار دارد، برنامه‌ی کاربردی باید گزاره‌ها (ادعاها)ی اولیه از مانده‌ی حساب، طبقه‌ی معاملات یا افشا را دربرگیرد. آیا برنامه‌ی کاربردی شامل کنترل‌های مناسب مربوط به ادعاهای اولیه‌ی مانده‌ی حساب نهایی یا طبقه‌ی معاملات است؟ در صورت کاربرد،

حسابرس فناوری اطلاعات باید برنامه‌ی کاربردی را در برابر ادعاهای مناسب آزمون کند. برای مثال، اگر ادعا مربوط به صحت است، آزمون ممکن است دربرگیرنده‌ی موارد زیر باشد:

- کنترل‌های اعتبار سنجی داده‌های ورودی
- محاسبات خودکار
- مغایرت‌گیری‌های خودکار

ادعای وجود ممکن است برای کنترل‌های اعتبارسنجی ورود داده‌ها آزمون شود. آزمون ادعای کامل‌بودن ممکن است برای کنترل‌های پردازش دسته‌ای یا مغایرت‌گیری‌های سفارشی انجام شود.

(۹) توجه به ابزارهای سودمند

بعضی ابزارهای مفید برای آزمون برنامه‌های کاربردی، فنون حسابرسی به کمک رایانه (CAATs) و ETLها هستند. فنون حسابرسی به کمک رایانه در اجرای روش‌هایی مثل داده‌کاوی مفید هستند- که نتایج داده‌ها را از ارسال توسط برنامه‌ی کاربردی بررسی می‌کند تا تعیین کنند که آیا کنترل‌های برنامه‌ی کاربردی کار می‌کنند، آیا برنامه‌ی کاربردی درست کار می‌کند و آیا برنامه‌ی کاربردی خطایی تولید کرده است. فنون حسابرسی به کمک رایانه همچنین در تجزیه و تحلیل داده‌ها برای اهدافی مانند درستی داده‌ها مفید است.

ETL در کشف داده‌های ناقص مفید است که می‌تواند با ردیابی رو به عقب به برنامه‌ی کاربردی تولیدکننده‌ی آن صورت گیرد و سپس برای اصلاح نقص در برنامه‌ی کاربردی فرصت فراهم سازد.

آزمون کنترل‌ها

بعضی از آزمون‌های کنترلی ممکن عبارت‌اند از:

- مغایرت‌گیری
- محاسبه‌ی مجدد
- تکرار
- شکاف

یک نمونه از مغایرت‌گیری ممکن است تطبیق‌دادن شناسه‌ی مشتری در پرونده‌ی معاملات با شناسه‌ی همان مشتری در پرونده‌ی اصلی باشد. به این معنی که آیا نام مشتری که در پرونده‌ی معاملات وجود دارد واقعا در فهرست مربوط به مشتریان مجاز هم هست یا نه؟ نمونه‌ی دیگر مربوط به محاسبه‌ی مجدد است؛ حسابرس فناوری اطلاعات ممکن است پایگاه داده‌ی مربوط به موجودی کالا را بررسی کند تا مطمئن شود آیا هزینه‌های کل موجودی کالا با جمع کنترلی در دفتر کل (مانده‌ی حساب) مطابقت دارد یا نه؟ تکرارها و شکاف‌ها هم در کشف خطاهای موجود در پردازش داده‌ها مفید هستند.

فنون حسابرسی به کمک رایانه

فنون حسابرسی به کمک رایانه می‌توانند در انجام مجدد محاسبات خودکار یا مغایرت‌گیری های خودکار استفاده شوند.

داده‌کاوی

داده‌کاوی می‌تواند در پشتیبانی از اهداف حسابرسی استفاده شود. به طور خاص در اجرای روش‌های محتوایی مربوط به فناوری اطلاعات مثل آزمون مصوبات و خطاهای طبقه‌بندی مربوط به کدهای مناسب مفید هستند.

آستانه‌های سفارش خرید

هر زمان که یک برنامه‌ی کاربردی شامل آستانه‌ای است که در آن مصوبه‌ی اولیه/ اضافی نیاز است، فنون حسابرسی به کمک رایانه در تعیین این که آیا آن کنترل به طور موثر کار می‌کند، مفید هستند. برای مثال، اگر برنامه‌ی کاربردی، سفارش‌های خرید یا پرداخت‌ها باشد و اگر خریدها و پرداخت‌ها یک به یک هستند (یعنی پرداخت‌ها بر اساس صورتحساب هستند و نه اظهارات)، یک آزمون ساده‌ی استخراج همه‌ی پرداخت‌های بالاتر از آستانه در مقابل پرونده‌ی داده‌ها که شامل مصوبات است (مثل پرونده‌ی سفارش خرید)، می‌تواند هر گونه استثنائاتی نسبت به کنترل/ آستانه را نشان دهد. این آزمون همچنین نفع دیگری در کشف تقلب دارد و آن زمانی است که کسی آستانه را عمدا زیر پا گذارد تا مرتکب تقلب شود.

نابهنجاری‌های موجودی کالا

اگر برنامه‌ی کاربردی مربوط به ثبت رسید دریافت موجودی کالا است، فنون حسابرسی به کمک رایانه می تواند برای نشان دادن این که آیا برنامه‌ی کاربردی اجازه‌ی ثبت مقادیر صفر یا منفی را می‌دهد یا نه، مورد استفاده قرار گیرد. بدیهی است، اگر اجازه‌ی این ثبت را بدهد، برنامه یک خطا (یا ناهنجاری) تولید کرده است. بنابراین، ضعف کنترلی دارد و نیاز به تغییر برنامه یا ایجاد کنترل جبرانی دارد. برنامه‌های کاربردی دیگری وجود دارند که آنها هم می‌توانند از این آزمون استفاده کنند.

دوم، اگر برنامه‌ی کاربردی مربوط به یک برنامه‌ی نگهداری فایل‌ها است، سامانه‌ی موقعیت‌هایی را که در آنها یک کارمند می‌تواند تغییراتی را در داده‌های موجودی کالا ایجاد کند و در نتیجه منجر به اختلافات و خطاهایی شود، به حداقل برساند.

برای جلوگیری از این نابهنجاری‌ها به کنترل‌هایی نیاز است. برای مثال، استفاده از منطق تفکیک مناسب وظایف می‌تواند دسترسی کارمندانی را که می‌توانند تغییراتی در فایل‌های نگهداری ایجاد کنند، محدود سازد. همچنین، برنامه‌ی کاربردی/سامانه می‌تواند از طریق ثبت داده‌ها قبل از تغییر و بعد از تغییر، تغییرات را ردیابی کند. بدون چنین ردیابی کارمندان می‌توانند تغییرات را تحریف کنند و خطاها یا تقلب در داده‌ها را ایجاد کنند. داده‌کاوی می‌تواند تفاوت‌های موجود در مانده‌ی حساب‌ها را با افزودن همه‌ی معاملات طی دوره به مانده‌ی ابتدای دوره و مقایسه‌ی آن با مانده‌ی پایان دوره کشف کند. وضعیت مشابهی برای هر برنامه‌ی کاربردی نگهداری فایل نوع وجود دارد.

(۱۰) تکمیل گزارش

به طور واضح همه‌ی حسابرسی‌ها با نوعی گزارش تمام می‌شود. این گزارش‌ها عموما شکل خاصی دارند. ولی در کل شامل اهداف حسابرسی، آزمون‌های انجام‌شده، نتایج آزمون‌ها (معمولا) و پیشنهادها می‌شوند.

نتیجه‌گیری

در سایه‌ی تروریسم جهانی و بحران‌های مالی شرکتی، حسابرسان فناوری اطلاعات به سرعت شالوده و دریانورد اصلی در واحد فناوری اطلاعات می‌شوند. در این مقاله به تفصیل ملاحظات خاص در مراحل یک حسابرسی برنامه‌ی کاربردی بیان شد. آن چه مهم است حسابرسی موفق برنامه‌ی کاربردی بستگی به وجود یک رویکرد قابل اتکا دارد. این مقاله رویکردی قابل اتکا و برخی ابزارهایی را نام برد که باید در انجام حسابرسی به خصوص مرحله‌ی نگاشت و فنون حسابرسی به کمک رایانه استفاده شوند.

در پایان باید اذعان داشت که ضروری است فناوری اطلاعات و کار حسابرسی در سازمان‌ها با هم در تعامل باشند تا شناخت بهتری از ریسک‌ها و کنترل‌ها به‌دست آید و اطمینان حاصل کرد که اهداف کسب‌وکار به طور کارا و اثربخش به‌دست محقق می‌شود.

پی‌نوشت:

1- Auditing of Application
2- Mapping
3- functionality
4- systems development life cycle (SDLC) controls
5- preaudit
6- Postaudits
7- Unified Modeling Language (UML)
8-commercial off-the-shelf software

منابع:

Bitterli, Peter R.)(2009). Integrated Auditing of IT Applications. EuroCACS 2009, Session 211.

SANS Institute.(2005).The Application Audit Process - A Guide for Information Security Professionals. SANS Institute Reading Room site.

Singleton, W. Tommie, (2012). Auditing Applications, Part 1. ISACA journal, Volume 3.

Singleton, W. Tommie, (2012). Auditing Applications, Part 2. . ISACA journal, Volume 4.

ابراهیم ابراهیمی: دانشجوی دکتری حسابداری دانشگاه تهران، دبیر فناوری مجله‌ی حسابدار، مدرس دانشگاه

مریم اشرفی: دانشجوی کارشناسی‌ارشد حسابداری دانشگاه شهید بهشتی