حسابرسی فناوری و ریسک عملیاتی

حامد فلامرزی
(دانشجو دکترای حسابداری- دانشگاه آزاد واحد سیرجان- ایران hamed.falamarzi2013@gmail.com)

ملیحه مجیدی
(کارشناس ارشد حسابداری- دانشگاه آزاد شیراز- ایران ma.majidi2013@gmail.com)

حسین هوشیارزاده
(دانشجوی کارشناس ارشد حسابداری- دانشگاه آزاد شیراز- ایران houshyarzadeh@gmail.com)

چکیده

با پیدایش کامپیوتر،دنیا به سرعت در حال تغییر بوده و عملیاتهای کسب و کار نیز به واسطه بهبود مداوم فناوری با سرعت فراوانی در حال تغییر هستند.گزارشهایی در خصوص دزدی اطلاعات،کلاهبرداران کامپیوتری،سوء استفاده از اطلاعات و سایر دغدغه های کنترل فناوری اطلاعات به کرات در اطراف جهان شنیده می شوند.سازمانها به لحاظ اطلاعاتی هشیارتر بوده،افراد به دلیل تمرکز زدایی پراکنده شده و کامپیوتر ها در کلیه حوزه های تجاری به طور کسترده ای استفاده می شوند.به دلیل گستردگی سریع فناوری های کامپیوتری و آسان بودن دسترسی به اطلاعات،حسابرسان IT آموزش دیده و ماهر در کار لازم است تا اطمینان حاصل شود که کنترل های موثری برای حفظ یکپارچگی داده ها و مدیریت دسترسی به اطلاعات قرار داده می شوند.همچنین آنها باید با محیط عملیاتی برای ارزیابی اثر بخشی کنترل های داخلی آشنا شده و شناخت لازم را از آن بدست آورند.نهایتا ،حسابرس فناوری اطلاعات باید پیچیدگی های فناوری سیستم های موجود و آتی و مواردی را که بر روی عملیاتها و تصمیم ها در کلیه سطوح تاثیر می گزارند را درک نماید.از اینرو در این مقاله قصد داریم به بررسی ضرورت حسابرسی فناوری اطلاعات پرداخته و جوانب ریسک های عملیاتی و مشخصه های لازم برای موفقیت نسبتا جدید را توصیف و تحلیل نماییم.

واژگان کلیدی:حسابرسی فناوری اطلاعات،ریسک های عملیاتی،اطمینان بخشی اطلاعات،کنترل،مشخصه های حرفه ای

۱- مقدمه

حسابرسی فناوری اطلاعات[۱] (IT) تحت عنوان حسابرسی پردازش داده‌های الکترونیکی[۲] (EDP) آغاز شد و با رشد فناوری در سیستمهای حسابداری ضرورت کنترل IT و تأثیر کامپیوترها روی ارائه خدمات تصدیقی[۳] به مقدار فراوانی توسعه پیدا کرد. چند سال گذشته به دلیل رسوایی‌های حسابداری و افزایش قوانین و مقررات، یک دوره محرک در دنیای حسابرسی IT بوده است. حسابرسی فناوری یک تاریخچه نسبتاً کوتاه ولی در عین حال غنی در مقایسه با کل حسابرسی داشته است و حوزه‌ای است که همواره در حال تغییر و تحول باقی می‌ماند. با ورود فناوری کامپیوتری به سیستمهای حسابداری، شیوه‌ای که داده‌ها ذخیره، بازیابی و کنترل می‌شدند، دچار تغییر و تحول شد. به نظر می‌رسد که اولین بار جنرال الکتریک در سال ۱۹۵۴ از یک سیستم حسابداری کامپیوتری شده استفاده نمود. در طول دوره زمانی ۱۹۵۴ تا اواسط دهه ۱۹۶۰ حرفه حسابرسی هنوز حسابرسی پیرامون کامپیوتر بود. در آن زمان تنها کامپیوترهای بزرگ[۴] استفاده می‌شد و افراد اندکی مهارتها و قابلیتهای برنامه‌نویسی کامپیوتری را داشتند. این روند در اواسط دهه ۱۹۶۰ با معرفی ماشینهای جدید، کوچکتر و ارزانتر شروع به تغییر نمود. این موضوع با استفاده از کامپیوترها در کسب و کارها افزایش یافت و در ادامه ضرورت آشنایی حسابرسان با مفاهیم EDP در کسب و کارها به وجود آمد. همراه با افزایش استفاده از کامپیوتر، ارتقاء در انواع مختلف سیستمهای حسابداری پدیدار شد. صنعت به سرعت متوجه شد، لازم است که نرم افزار خود را توسعه دهند و اولین نرم افزار حسابرسی تعمیم یافته[۵] (GAS) تولید شد. در سال ۱۹۶۸، انجمن حسابداران رسمی آمریکا[۶] (AICPA)، هشت شرکت (اکنون چهار شرکت) حسابداری بزرگ داشت که در توسعه حسابرسی EDP مشارکت می‌کردند. به علاوه، در همین دوره زمانی، حسابرسان EDP، انجمن حسابرسان پردازش داده‌های الکترونیکی[۷] (EDPAA) را تشکیل دادند .

همچنین، ضرورت وجود کنترلهای بهتر روی IT پیش از این از طریق مطالعات انجام شده توسط کمیته سازمانها مسؤول کمیسیون تردوی[۸] (COSO) متعلق به AICPA، ایزو ۹۰۰۰، «گزارش کنترل و قابلیت حسابرسی سیستمها[۹] (SAC)» متعلق به انجمن حسابرسان داخلی[۱۰] (IIA)، رهنمودهایی برای امنیت IS توسط سازمان همکاری و توسعه اقتصادی[۱۱] (OECD) و شورای رئیس جمهوری ایالات متحده در حوزه یکپارچگی و کارایی[۱۲] در برنامه آموزش حسابرسی کامپیوتری منعکس شده است. دیگر الحاقات به این مطالعات عمده، استراتژی ملی برای امنیت فضای سایبری[۱۳] متعلق به ایالات متحده منتشر شده در سال ۲۰۰۲ و ایزو ۱۷۷۹۹ و اصلاحیه‌های دنبال آن هستند. به علاوه، در سال ۱۹۹۴، EDPAA نامش را به انجمن کنترل و حسابرسی سیستمهای اطلاعاتی[۱۴] (ISACA) تغییر داد. هدف انجمن ایجاد رهنمودها، رویه‌ها و استانداردهایی برای حسابرسان EDP بود. COSO، نیز در سال ۱۹۹۷، چارچوب یکپارچه‌ای را برای کنترل داخلی به طور خاص برای کنترلهای IT به چاپ رساند. از جمله دیگر شناخته شده‌ها SAC متعلق به IIA و COBIT متعلق به ISACA هستند که هر دو مستقیماً با چارچوبهای شناسایی شده توسط COSO در ارتباط هستند [۱۳]. به طوری که، اولین نسخه از اهداف کنترلی در سال ۱۹۷۷ چاپ شده بود. اکنون این کتاب تحت عنوان چارچوب اهداف کنترلی برای اطلاعات و فناوری مرتبط با آن[۱۵] (COBIT) مشهور است که نسخه اول آن در سال ۱۹۹۶ توسط انجمن نظام راهبری (حاکمیت) IT[۱۶] (ITGI) که تحت نظارت ISACA در حوزه IT فعالیت می‌کند، به چاپ رسیده و نسخه ۴.۱ آن نیز به عنوان آخرین نسخه تجدیدنظر شده‌اش در ماه می سال ۲۰۰۷ توسط همین انجمن ارائه شده بود. COBIT، در سطحی بالا قرار می‌گیرد و به منظور دقت بیشتر با شیوه‌های مناسب و استانداردهای IT همچون COSO، ITIL، ISO 27000، CMMI، TOGAF و PMBOK تنظیم و هماهنگ شده است. همچنین، COBIT 5 برای ارائه در سال ۲۰۱۲ زمانبندی شده بود که به تازگی در آوریل ۲۰۱۲، توسط به نام خود ISACA و نه تحت نام ITGI به چاپ رسید. COBIT 5 به یکپارچگی COBIT 4.1، Val IT 2.0 و چارچوبهای Risk IT پرداخته است و همچنین، به میزان قابل توجهی مدل کسب و کار برای امنیت اطلاعات[۱۷] (BMIS) و چارچوب اطمینان بخشی فناوری اطلاعات[۱۸] (ITAF) را ترسیم می‌کند. COBIT، به طور کلی مجموعه‌ای از اهداف کنترلی پذیرفته شده IT برای حسابرسان IT است. شکل‌گیری و پیشروی

در رواج اینترنت و تجارت الکترونیک نیز تأثیرات قابل توجهی بر روی رشد حسابرسی IT داشته است. اینترنت بر روی زندگی اکثر مردم جهان تأثیرگذار بوده و محلی برای ارتقاء کسب و کار، سرگرمی و جرم است. حسابرسی IT به سازمانها و افراد کمک می‌کند که بر روی اینترنت به امنیت دست یابند، در حالیکه تجارت و ارتباطات خود را رشد می‌بخشند. در سالهای آتی، حسابرسی بدون کاغذ متداول خواهد شد؛ چون مشتریان به طور روزافزونی از سیستمهای اطلاعاتی بدون کاغذ استفاده می‌کنند و نرم افزارهای حسابرسی به وجود خواهند آمد که به حسابرسان امکان حسابرسی آنی را می‌دهند. استفاده از فناوریهای نوین، حسابرس را از بسیاری وظایف خسته و کسل کننده رهایی خواهد بخشید و به او اجازه خواهد داد که وقت خود را صرف وظایف مهمتر دیگری کند. برخی از انواع خدمات حسابرسی و اطمینان بخشی در محیط تجارت الکترونیک شامل: تحلیل ریسک، انتخاب و تعدیل سیستم تجارت الکترونیک، خدمات ارایه شده به مشتریان، بررسی امنیت سیستم تجارت الکترونیک، حسابرسی آنی، نگهداری و حفاظت از سیستمهای تجارت الکترونیک، حسابرسی کنترلهای داخلی و حسابرسی مستمر است .

در این مقاله قصد داریم به مرور، معرفی و تحلیل جنبه‌های مختلف حسابرسی فناوری اطلاعات و ریسک های عملیاتی بپردازیم. به طوری که، دلایل موجود برای ضرورت انجام حسابرسی فناوری اطلاعات در این عصر را بیان می‌کنیم. سپس، در خصوص نقشهای مختلفی که یک حسابرس IT می‌تواند ایفاء نماید، بحث می‌نمایم. همچنین، انواع کنترلهای لازم در زمینه فناوری اطلاعات ،ضرورت ونقش فناوری اطلاعات وریسک های عملیاتی را تشریح نموده ودرپایان، نتیجه‌گیری انجام می‌شود.

۲- حسابرسی و فناوری اطلاعات

حسابرسی فرآیندی است منظم و با قاعده (سیستماتیک) جهت جمع‌آوری و ارزیابی بی طرفانه شواهد درباره ادعاهای مربوط به فعالیت‌ها و وقایع اقتصادی، به منظور تعیین درجه انطباق این ادعاها (اظهارات) با معیارهای از پیش تعیین شده و گزارش نتایج به افراد ذینفع. ورود فناوری اطلاعات در عرصه مالی، حرفه حسابرسی را نیز تحت تأثیر قرار داده است. حسابرسان با استفاده از این ابزار جدید قادر به تحلیل و پردازش حجم انبوه اطلاعات در حداقل زمان و با کیفیت بالا هستند. فنون رایانه‌ای حسابرسی، به حسابرسان امکان می‌دهد عملیات حسابرسی را به طور اثر بخش اجرا کنند که این امر، موجب ارتقای کارایی، بهره‌وری و کیفیت حسابرسی می‌شود.

حسابرسان فناوری اطلاعات، اغلب خود را در حال آموزش جامعه تجاری در این زمینه می‌بینند که کار آنان چگونه بر ارزش سازمان می‌افزاید. بخش‌های حسابرسی داخلی به طور معمول دارای یک زیر گروه حسابرسی فناوری اطلاعات است که با چشم‌اندازی روشن از نقش خود در سازمان، به کار گمارده شده‌اند. اگر چه طبق تجربه به دست آمده به عنوان حسابرس فناوری اطلاعات، هر چه جامعه تجاری گسترده‌تر باشد. برای دستیابی به حداکثر سود به شناخت بیشتر کارکرد حسابرسی فناوری اطلاعات نیازمند است. در این نوشتار، منافع ویژه و ارزش افزوده حاصل از حسابرسی فناوری اطلاعات، به طور مختصر بررسی شده است. در معنای خاص، حسابرسی فناوری اطلاعات، به طور مختصر بررسی شده است. در معنای خاص، حسابرسی فناوری اطلاعات ممکن است طیفی گسترده از زیر ساخت‌های پردازش و ارتباطات فناوری اطلاعات مانند سیستم‌ها و شبکه‌های مشتری- خدمت رسان، سیستم‌های عامل، سیستم‌های امنیتی، نرم افزارهای کاربردی، خدمات شبکه جهانی، پایگاه‌های داده، زیر ساخت‌های مخابراتی، روش‌های مدیریت تغییر و برنامه‌ریزی

برای رویارویی با حوادث مترقبه را پوشش دهد. توالی کار در یک حسابرسی استاندارد با شناسایی خطرها آغاز و سپس با ارزیابی ساختار کنترل‌ها ادامه و با آزمون اثر بخشی کنترل‌ها پایان می‌یابد. حسابرسان با مهارات، می‌توانند در هر مرحله از حسابرسی موجب افزایش ارزش شوند شرکت‌ها به طور معمول از کارکرد حسابرسی فناوری اطلاعات، برای فراهم ساختن اطمیناتن از کنترل‌های فناوری و اطمینان از انطباق با الزامات خاص قانونی با صنعت، استفاده می‌کنند با رشد سرمایه‌گذاری در فناوری اطلاعات، حسابرسی فناوری اطلاعات می‌تواند اطمینان دهد که خطرها کنترل می‌شود و احتمال زیان‌هایی بزرگ وجود ندارد. سازمان نیز ممکن است خود تشخیص دهد که خطر توقف، تهدید امنیتی یا آسیب‌پذیری بالاست. همچنین ممکن است الزاماتی برای رعایت مفاد قانون مانند قانون ساربینز- اکسلی یا الزامات خاص صنعت وجود داشته باشد. در ادامه در رابطه با پنج حوزه کلیدی بحث می‌شود که از طریق آن‌ها، حسابرسان فناوری اطلاعات می‌توانند به ارزش است.

دامنه طرح‌ریزی شده برای حسابرسی نیز در افزودن ارزش، مهم است. بدون یک تعهد روشن در مورد این که چه فرآیندها و خطرهای تجاری، حسابرسی خواهد شد، اطمینان از دستیابی به موفقیت یا افزودن ارزش، دشوار است.

بنابراین، در اینجا پنج روش افزودن به ارزش‌های سازمان از طریق حسابرسی فناوری اطلاعات، ارائه می‌شود:

الف) کاهش خطر:

برنامه‌ریزی و اجرای حسابرسی فناوری اطلاعات دربرگیرنده شناخت و برآوردخطرها در سازمان است. حسابرسی‌ها فناوری اطلاعات به طور معمول خطرهای مرتبط با اعتمادپذیری، یکپارچگی و دسترس‌پذیری زیر ساخت‌ها و فرآیندهای فناوری اطلاعات را پوشش می‌دهد. خطرهای دیگر شامل اثر بخشی، کارایی و اتکاپذیری فناوری اطلاعات است. نخستین بار که خطر برآورد شود، می‌توان به چشم اندازی روشن از این دست یافت که برای کاهش به تخفیف خطر از طریق به کارگیری کنترل، انتقال خطر از طریق بیمه، یا به طور ساده پذیرفتن خطر به عنوان بخشی از محیط عملیاتی، چه مسیری در نظر گرفته شود. یک فرض مهم در این جا این است که خطر فناوری اطلاعات، خطر کسب و کار تجاری است. هر گونه تهدید یا آسیب‌پذیری عملیات اصلی فناوری اطلاعات، ممکن است اثری مستقیم بر کل سازمان داشته باشد. به طور خلاصه، سازمان نیاز دارد بداند که خطرها در کجا هستند و سپس اقدام به انجام کاری در مورد آن‌ها کند. بهترین رویه‌های به کار گرفته شده در مورد خطر فناوری اطلاعات از سوی حسابرسان، چارچوب کوبیت (COBIT) طراحی شده توسط انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی و چارچوب خطر سیستم‌های اطلاعاتی و استاندارد اقدامات عملی مدیریت امنیت اطلاعات است.

ب)تقویت کنترل‌ها (و بهبود امنیت)

پس از برآورد خطرهای پیشگفته، سپس می‌توان کنترل‌ها را مشخص و ارزیابی کرد و کنترل‌هایی که طراحی ضعیف یا غیر مؤقر دارند را می‌توان دوباره طراحی و یا تقویت کرد. چارچوب کوبیت در رابطه با کنترل‌های فناوری اطلاعات به ویژه در اینجا مفید است. این چارچوب شامل چهار قلمرو سطح بالا است که ۳۲ فرآیند کنترل سودمند در زمینه کاهش خطر را پوشش می‌دهد.

چارچوب کوبیت همه جنبه‌های امنیت اطلاعات از جمله هدف‌های کنترل‌ها، شاخص‌های کلیدی عملکرد، شاخص‌های کلیدی هدف و عوامل مهم موفقیت را پوشش می‌دهد. حسابرس می‌تواند چارچوب کوبیت را برای ارزیابی کنترل‌ها در یک سازمان به کار گیرد و

پیشنهادهایی ارائه دهد که بر ارزش واقعی محیط فناوری اطلاعات و سازمان در کل، بیفزاید. یکی دیگر از چارچوب‌های کنترل، مدل‌های کنترل داخلی کمیته سازمان‌های حامی کمیسیون تردوی یا کوزو (COSO) است. حسابرسان فناوری اطلاعات می‌توانند این چارچوب را برای اطمینان یافتن از ۱) اثر بخشی و کارایی عملیات، ۲) اتکاپذیری گزارشگری مالی و ۳) رعایت قوانین و مقررات لازم الاجرا، به کار گیرند. این چارچوب، دو عنصر از پنج عنصری که به طور مستقیم به کنترل‌ها مربوطند یعنی محیط کنترلی و فعالیت های کنترلی را در بر می‌گیرد.

ج) رعایت مقررات

مقررات گسترده در سطح دولت مرکزی و ایالتی، الزامات خاصی را برای امنیت اطلاعات در بر می گیرد. حسابرس فناوری وظیفه‌ای حیاتی دارد که اطمینان دهد الزامات خاص رعایت، خطرها برآورد و کنترل‌ها به کار گرفته شده است. قانون ساربینز- اکسلی (قانون پاسخگویی شرکت و جرایم تقلب) الزامات مورد نیاز برای تمام شرکت‌های سهامی عام به منظور اطمینان یافتن از کفایت کنترل‌های داخلی طبق تعریف ارائه شده در چارچوب کمیته سازمان‌های حامی کمیسیون تردوی(کوزو) را در بر می‌گیرد. حسابرس فناوری اطلاعات است که اطمینان می‌دهد که چنین الزاماتی رعایت شده است، قانون پاسخگویی و انتقال‌پذیری بیمه بهداشتی دارای سه حوزه الزامات فناوری اطلاعات شامل اداری، فنی و عینی می‌باشد. حسابرس فناوری اطلاعات است که در اطمینان یافتن از رعایت این الزامات، نقشی کلیدی دارد. صنایع گوناگون الزامات دیگری دارند از جمله، استاندارد امنیت داده‌ها در صنعت کارت پرداخت در صنعت کارت‌های اعتباری، مانند ویزا و مسترکارت. در تمام حوزه‌های رعایت قانون و مقررات، حسابرس فناوری اطلاعات نقشی محوری بازی می‌کند. سازمان نیاز دارد اطمینان یابد که همه الزامات رعایت شده است.

د)تسهیل ارتباط بین مدیریت کسب و کار تجاری و مدیریت فناوری

حسابرسی می‌تواند در گشایش کانال‌های ارتباطی میان مدیریت کسب و کار و مدیریت فناوری سازمان، تأثیر مثبت داشته باشد. حسابرسان از آنچه در واقعیت و در عمل روی می‌دهد. مصاحبه، مشاهده و آزمون به عمل می‌آورند.

نتیجه نهایی حسابرسی، اطلاعاتی ارزشمند به شکل گزارش‌های کتبی و شفاهی است. مدیریت ارشد می‌تواند درباره چگونگی کارکرد سازمان خود، بازخورد مستقیم دریافت کند. کارشناسان حرفه‌ای فناوری در سازمان همچنین نیازمندند که انتظارات و هدف‌های مدیریت ارشد را بدانند. حسابرسان از طریق شرکت در نشست‌هایی با مدیریت فناوری و از طریق بررسی نحوه کنونی اجرای سیاست‌ها، استانداردها و رهنمودها به این نوع ارتباط از بالا به پایین، کمک می‌کنند. درک این موضوع مهم است که حسابرسی فناوری اطلاعات یک عنصر کلیدی در نظارت مدیریت بر فناوری است. فناوری سازمان به این دلیل وجود دادر که از راهبرد، کارکردها و عملیات کسب و کار پشتیبانی کند. همسویی کسب و کار با فناوری پشتیبان آن، بسیار مهم است. حسابرسی فناوری اطلاعات، این همسویی را حفظ می‌کند.

ر)بهبود نظام راهبری فناوری اطلاعات:

مؤسسه حسابرسی جهانی فناوری اطلاعات تعاریف زیر را منتشر کرده است: مسئولیت نظام راهبری فناوری اطلاعات، بر عهده مدیران اجرایی هئیت مدیره است و در برگیرنده راهبری، ساختارها و فرآیندهای سازمانی است تا اطمینان دهد که فناوری اطلاعات سازمان، راهبردها و هدف‌های سازمان را حفظ کرده و گسترش می‌دهد. «در تعریف یاد شده از راهبری، ساختارها و فرآیندهای سازمانی، همه جا به حسابرسان فناوری اطلاعات به عنوان بازیگران کلیدی اشاره شده است. موضوع محوری درحسابرسی فناوری اطلاعات، و در کل مدیریت فناوری اطلاعات، شناخت قوی ارزش‌ها، خطرها وکنترل‌های پیرامون محیط فناوری سازمان می‌باشد. به گونه‌ای دقیق‌تر، حسابرسان فناوری اطلاعات، ارزش‌ها، خطرها و کنترل‌ها در هر یک از اجزای اصلی فناوری مانند برنامه‌های کاربردی، اطلاعات، زیر ساخت‌ها و اشخاص را بررسی می‌کنند.

نگرشی دیگر درباره نظام راهبری فناوری اطلاعات متشکل از چارچوبی در بر گیرنده چهار هدف کلیدی است که در مستندات مؤسسه حسابرسی فناوری اطلاعات مورد بحث قرار گرفته است:

- فناوری اطلاعات با کسب و کار همسو است.

- فناوری اطلاعات، کسب و کار را توانمند می‌سازد و سود را به حداکثر می‌رساند.

- منابع فناوری اطلاعات به گونه‌ای مسئولانه به کار گرفته می‌شود.

- خطرهای فناوری اطلاعات به گونه‌ای مناسب مدیریت می‌شود.

حسابرسان فناوری اطلاعات اطمینان فراهم می‌کنند که هر یک از این هدف‌ها، تحقق یافته است. هر هدف برای سازمان مهم است و بنابراین، در عملیات حسابرسی فناوری اطلاعات اهمیت دارد.

۲-۱- انواع حسابرسی فناوری اطلاعات

۲-۱-۱ حسابرسی پردازش نوآوری‌های فناوری:

- هدف این حسابرسی طرح‌ریزی شکلی از ریسک برای پروژه‌های موجود و آینده است.

۲-۱-۲- حسابرسی مقایسه‌ای نوآوری‌ها:

- شکل دیگری از حسابرسی فناوری اطلاعات، حسابرسی مقایسه‌ای نوآوری‌هاست. این حسابرسی همان‌طور که از نامش پیداست. به معنای انجام دادن تجزیه و تحلیل توانایی‌های نوآوری و ابداعات شرکت‌های مورد حسابرسی در مقایسه با سایر رقیبان شرکت‌هاست.

۲-۱-۳-حسابرسی وضعیت فناوری:

- شکل سوم حسابرسی فناوری اطلاعات، حسابرسی وضعیت فناوری است. این حسابرسی نیز فناوری‌هایی را که در حال حاضر در شرکت وجود دارد و فناوری‌هایی را که شرکت نیاز دارد تا به آن دست یابد، بررسی می‌کند.

۲-۲- اهمیت کنترل و حسابرسی فناوری اطلاعات

از مهمترین عواملی که منجر به لزوم انجام حسابرسی فناوری اطلاعات شدند بشرح زیر می‌باشند:

- حسابرسان متوجه تواناییهای نهفته در سیستم‌های کامپیوتری برای انجام عملکرد گواهی دادن شدند.
- شرکتها پردازش و مدیریت اطلاعات را در سازمان خود به رسمیت شناختند بطوریکه رایانه‌ها 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.
- انجمن‌های حرفه‌ای و سازمان‌ها و نهادهای نظارتی دولتی نیاز به کنترل و حسابرسی فناوری اطلاعات را به رسمیت شناختند.

بنابراین حسابرسی فناوری اطلاعات بخشی جدایی‌ناپذیر از تابع حسابرسی است، زیرا پشتیبانی از قضاوت حسابرس در کیفیت پردازش اطلاعات توسط سیستم‌های کامپیوتری را بر عهده دارد. بطوریکه در ابتدا، به عقیده حسابرسان، مهارتهای حسابرسی فناوری اطلاعات به عنوان منابع تکنولوژیکی برای کارکنان حسابرسی به شمار می‌آمد. کارکنان حسابرسی اغلب به این منابع برای کمک‌های فنی نگاه میکرند.

۲-۳- بعد جدیدی به نام اطمینان بخشی اطلاعات

امروزه، سازمانها در برنامه‌ریزی، هدایت، هماهنگی و اجرای عملیاتها به شدت به قابلیتهای اطلاعات الکترونیکی دیجیتالی خود برای ذخیره‌سازی، پردازش و جابجایی داده‌های ضروری اتکا می‌کنند. لیکن، تهدیدهای قوی و پیچیده می‌توانند از نقاط ضعف امنیتی در بسیاری از این سیستمها بهره‌برداری نمایند. با برون سپاری توسعه تکنولوژیکی به کشورهایی که تروریستهایی را در ستاد توسعه‌شان دارند، احتمال آن وجود دارد که کد اجرا شده موجب خرابی، اختلاس، دزدی و غیره شود. این قبیل موضوعات و سایر نقاط ضعفی را که می‌توان به عنوان نقاط آسیب‌پذیر استخراج نمود، می‌توانند حساسترین اجزای قابلیتهای اطلاعاتی سازمان را به خطر بیاندازند. اگر چه، می‌توان دفاعهای لایه‌ای و عمیقی را برای کاهش آسیب‌پذیریها و جلوگیری، مقابله و ترمیم بسیاری از تهدیدها به کار برد. از جنبه اطمینان بخشی اطلاعات[۲۷] (IA)، قابلیتهایی که باید از آنها دفاع شود را می‌توان بر حسب چهار عنصر عمده به میزان گسترده‌ای مشاهده نمود: محیطهای محاسباتی محلی، مرزهایشان، شبکه‌هایی که آنها را به یکدیگر پیوند می‌دهند و زیرساخت پشتیبانی آنها. استراتژی ملی ایالات متحده برای امنیت فضای سایبری یکی از آن ابتکارات است.

اصطلاح «اطمینان بخشی اطلاعات» در قالب بی‌نقصی اطلاعات (سطح اطمینان و اعتمادی که می‌توان به اطلاعات داشت) و دسترس‌پذیری خدمت تعریف می‌شود. در کلیه متون، خواه کسب و کاری یا دولتی، به معنای محافظت از مجموعه، ذخیره‌سازی، ارسال و استفاده از اطلاعات است. هدف نهایی اطمینان بخشی اطلاعات، پشتیبانی از کاربران، واحدهای کسب و کار و سازمانها در

مقابل تأثیرات منفی تحریف اطلاعات یا ممانعت از ارائه خدمات است. باور بر این است که دپارتمان سازمانهای پشتیبانی و امنیتی homeland همچون آژانس امنیت ملی، دیوان رسیدگی فدرال[۲۸] (FBI) و آژانس جاسوسی مرکزی[۲۹] (CIA) برای پشتیبانی این هدف و برنامه کار کرده‌اند. دامنه چنین نمونه‌هایی را می‌توان به حالتی که داده‌های پرسنلی در یک پایگاه داده منابع انسانی معتبر است، محدود نمود. به این معنی که می‌توانست باشد اما در واقع نیست، لیکن، هیچ تأثیر منفی روی IS نمی‌تواند داشته باشد، اما زمانیکه افراد مقداری پول را با اشتباه در چکهای پرداختی‌شان دریافت می‌کنند یا زمانیکه پول به نشانی نادرستی ارسال می‌شود، سازمان ممکن است زیان ببیند. به طور مشابه، اگر سفارش برای یک قطعه موتوری در بخشی از سیستم لجیستیک و تأمین که باید دستور بدهد که پالتها روی قایق به سمت مقصد بارگذاری شوند، مفقود شود، IS به عملیات ادامه می‌دهد، اما ارائه خدمت به شخص نیازمند قطعات اتفاق نمی‌افتد. به صورت طبیعی، اگر پردازش، ذخیره‌سازی یا ارتباطات اطلاعاتی IS خراب یا غیر قابل دسترس شود، به طور کلی، سازمان نیز تأثیرپذیر خواهد شد. هر چند، حقیقتاً پشتیبانی سیستمها بدون پشتیبانی اطلاعات، پردازش و ارتباطات کافی نیست. همچنانکه IS ملی و زیرساختارهای حیاتی آنها (دولت و کسب و کار) به یکدیگر متصل می‌شوند، نقاط ورودی و در معرض‌گذاری افزایش یافته و از اینرو، ریسکها افزایش می‌یابند .

۲-۳- حسابرس IT و نقش آن در هزاره جدید

امروزه، حسابرسان IT با مدیران، کاربران و تکنسینهای بسیاری از سازمانها در حوزه‌های مختلف تعامل دارند. آنها باید دارای مهارتهای بین فردی برای تعامل با سطوح چندگانه پرسنل و دارای مهارتهای فنی برای درک فناوریهای مختلف مورد استفاده در فعالیت پردازش اطلاعات (به ویژه فناوری که روی صورتهای مالی شرکت تأثیر می‌گذارد) باشند. همچنین، متخصص این کار باید درک و آشنایی لازم با محیط عملیاتی را برای ارزیابی اثربخشی کنترل داخلی کسب نماید. در نهایت، حسابرس IT باید پیچیدگی‌های فناوریهای موجود و سیستمهای آتی و مواردی را که بر روی عملیاتها و تصمیمات در کلیه سطوح تأثیر می‌گذارند، درک نماید. حسابرس IT در فرایند وارسی یکپارچگی سیستمهای مبتنی بر کامپیوتر درگیر می‌شود. این فرایند شامل بررسی، آزمون و ارزیابی کنترلهای داخلی درون و پیرامون سیستمهای مبتنی بر کامپیوتر می‌شود. حسابرس IT یک متخصص نسبتاً جدید است. فرصتهای استخدامی برای حسابرسی IT در کلیه بخشهای صنایع خصوصی، حسابداری رسمی و دولتی سرتاسر جهان ارائه می‌شوند.

از اینرو، پهنا و عمق دانش مورد نیاز برای حسابرسی IT وسیع است. حسابرسی IT با نرم افزار کاربردی رویکردهای حسابرسی ریسک‌گرا؛ استفاده از ابزار و تکنیکهای حسابرسی به کمک کامپیوتر (به طور مثال، EnCase، Case Ware، Idea، ACL، Guardant، e Trust، CA-Examine)؛ نرم افزار کاربردی استانداردها (ملی یا بین‌المللی) همچون ایزو ۹۰۰۰/۳ و ایزو ۱۷۷۹۹ و الحاقات مرتبط برای بهبود و اجرای سیستمهای کیفیت در توسعه نرم افزار؛ حسابرسی سیستمهای تحت توسعه شامل دوره عمر توسعه سیستمهای[۳۰] (SDLC) پیچیده یا تکنیکهای توسعه جدید (به عنوان مثال، پیش نمونه‌سازی،[۳۱] محاسبات کاربر نهایی،[۳۲] توسعه سیستمهای سریع)؛[۳۳] و حسابرسی فناوریهای پیچیده شامل تبادل داده‌های الکترونیکی، سرورهای مشتری، شبکه‌های منطقه‌ای گسترده و محلی، ارتباطات داده‌ای، ارتباطات از راه دور و سیستمهای صدا/ داده/ تصویر یکپارچه سر و کار دارد. سایر حوزه‌های ذکر شده برای پیشرفت در آینده، تجارت الکترونیک، سنجش عملکرد درمان،[۳۴] تطبیق سیاست،[۳۵] حسابرسی داخلی برون سپاری شده،

ذیحسابی شریک تجاری،[۳۶] ادغامها و اکتسابات، ایزو ۹۰۰۰ و ادعاهای وب گسترده جهانی[۳۷] هستند. این موارد و حوزه‌هایی که پیش از این ذکر شد، نگاهی اجمالی از تأثیر فناوری روی فرایندهای کسب و کار و ضرورت اطمینان بخشی اطلاعات جهت حسابرسی، کنترل و ایمن‌سازی را ارائه می‌کنند.

۳- ضرورت حسابرسی فناوری

سازمانها به شدت به فناوری کامپیوتری وابسته شده‌اند. با افزایش اتکا به کامپیوترها برای انجام تراکنشهای روزانه و افزایش ریسکهای همراه با فناوری جدید، مدیریت تمایل دارد که از کفایت کنترلهای نظارتی بر عملیاتهای کامپیوتری اطمینان حاصل کند. مدیریت انتظار دارد که حسابرس این اطمینان را فراهم کند. اگر چه، به واسطه تحول سریع در فناوری و ریسکهای جدید همراه با آن فناوری، لازم است که متخصصان این ارزیابی‌های کنترلی را انجام دهند. بدین ترتیب، حسابرسان EDP گذشته به حسابرسان IT امروزی و آینده تبدیل شده‌اند. جدول ۱، ۱۰ دلیل مهم برای آغاز حسابرسی IT را نمایش می‌دهد.

امروزه، شرکتهای حسابدار رسمی[۳۸] (CPA) (فرانسه، انگلستان، آمریکا، ایتالیا) گروههای خاصی را طراحی کرده‌اند که در زمینه حسابرسی IT متخصص هستند. شرکتهای مسؤولیت محدود Price Waterhouse Coopers، Ernst & Young، Deloitte و KPMG دارای ستادهایی هستند که حسابرسیهای IT را انجام می‌دهند. اکثر این گروهها به حسابرسان مالی در تصدیق صحت صورتهای مالی برای شرکتهایی که در آنها حسابرسی انجام می‌دهند، کمک می‌کنند. بقیه روی پروژه‌های خاصی همچون امنیت اینترنتی در زمینه مطالعات نفوذ،[۳۹] ارزیابی‌های دیواره آتش،[۴۰] پلها،[۴۱] مسیریابها[۴۲] و پیکربندی‌های اتصال بین دو شبکه[۴۳] تمرکز می‌کنند.

جدول ۱: ۱۰ دلیل مهم برای آغاز حسابرسی فناوری

۱. حسابرسی روی کامپیوتر جهت کسب اطمینان نسبت به داده‌ها رضایتبخش نبود.
۲. اطمینان به کنترلها به شدت مشکوک شده بود.
۳. به دلیل خلاقیت در برنامه‌نویسی، مؤسسات مالی در حال پول از دست دادن بودند.
۴. به دلیل وجود برنامه‌نویسهای سطح بالا نمی‌توانستند به دقت پایگاه داده لیست حقوق اعتماد کنند.
۵. امنیت داده‌ها به صورت کارا اجرا نمی‌شد.

۶. پیشرفتهای به وقوع پیوسته در فناوری
۷. شبکه‌های داخلی توسط کامپیوترهای رومیزی کارکنان قابل دسترسی بودند.
۸. کامپیوترهای شخصی برای استفاده خانگی و دفتری دسترس‌پذیر شده بودند.
۹. حجم زیاد داده‌ها به برنامه‌های نرم افزاری پیشرفته برای حسابرسی نیاز داشت که تحت عنوان CAATs (تکنیک حسابرسی به کمک کامپیوتر)[۴۴] مشهور است.
۱۰. رشد عظیم هکرهای شرکتی چه داخلی یا خارجی، حکم به ضرورت وجود حسابرسان فناوری می‌کرد.

سایر حوزه‌هایی که لازم است حسابرس فناوری در آنها مهارت داشته باشد، در جدول ۲ فهرست می‌شوند.

۳-۱- نقش حسابرس فناوری

حسابرسی که سیستمهای پیچیده امروزی را ارزیابی می‌کند، باید به شدت مهارتهای فنی خود را برای درک روشهای استنتاجی پردازش اطلاعات توسعه دهد. سیستمهای معاصر[۴۵] ریسکهایی همچون بسترهای ناسازگار،[۴۶] روشهای جدید برای نفوذ به امنیت از طریق شبکه‌های ارتباطی (به عنوان مثال، اینترنت) و غیر متمرکزسازی سریع پردازش اطلاعات همراه با خسارت ناشی از کنترلهای متمرکز را به همراه دارند. حسابرسی محیط پردازش به دو بخش تقسیم می‌شود. اولین و فنی‌ترین بخش حسابرسی، ارزیابی محیط عملیاتی به وسیله بسته‌های نرم افزاری اصلی (به عنوان مثال، سیستمهای امنیتی و عامل) که به نمایندگی از کنترلهای محیطی یا عمومی در محیط پردازش خودکار شده است. این بخش معمولاً توسط متخصصان حسابرسی IT حسابرسی می‌شود. بخش دوم محیط پردازش نرم افزار کاربردی خودکار است که توسط حسابرس عمومی که دارای مهارتهای کامپیوتری است، حسابرسی می‌شود.

جدول ۲: مهارتهای مرتبط با حسابرسی فناوری

شماره	موضوع	شرح
۱	انجام کنترلهای عمومی	عملیاتهای داخلی و خارجی
۲	آماده‌سازی ارزیابی‌های نرم افزار کاربردی	مشخصه‌های روی سیستم اصلی،

		Unix، ویندوز NT و سایر سیستمهای عامل
۳	انتقال پروتکل کنترلی/ پروتکل اینترنتی[۴۷] (TCP/IP)	روش امنیتی داده‌های مرتبط با اینترنت
۴	روش انتقال غیر همزمان[۴۸] (ATM)	ارتباطات از راه دور
۵	انتقال الکترونیکی وجوه[۴۹] (EFT)	ارتباطات از راه دور
۶	سیستمهای مدیریت پایگاه داده[۵۰] (DBMS)	دانش اوراکل، اکسس و سایر DBMSها
۷	برنامه‌ریزی تداوم کسب و کار (برنامه‌ریزی ترمیم حادثه کامپیوتری)[۵۱]	برنامه‌ریزی و اجرای طرح پیشنهادی ترمیم حادثه کامپیوتری شرکت
۸	سیستمهای تحت تغییر	استفاده از متدلوژی توسعه سیستمی، طراحی امنیت و کنترل و بررسیهای پس از اجرا
۹	خدمات یکپارچه حسابرسی	کار با حسابرسان مالی برای ایجاد ادعاها روی صورتهای مالی شرکت
۱۰	خدمات امنیت اطلاعات	مطالعات نفوذ اینترنتی با استفاده از سیستمهای امنیت اینترنت[۵۲] (ISS)، ابزار مدیریت امنیت برای تحلیل شبکه‌ها[۵۳] (SATAN) و تنظیم مسأله بهینه‌سازی محدود[۵۴] (COPS) در مقیاس بزرگ و سایر ابزارهای امنیت اینترنت تجاری

به علاوه، کاربردهای جدید IT ریسکهای جدیدی را مطرح می‌کند که متقابلاً نیاز به کنترلهای جدیدی نیز دارند. حسابرسان فناوری نیز برای ارزیابی ارتباط سیستمی خاص با کل سازمان در موقعیت منحصر بفردی هستند. به همین دلیل، غالباً حسابرس فناوری در تصمیم‌گیری مدیر ارشد نقش بازی می‌کند. نقش حسابرس فناوری را می‌توان در طی فرایند نظام راهبری IT و استانداردهای موجود کار حرفه‌ای برای این حرفه بررسی نمود. همانطور که پیش از این ذکر شد، نظام راهبری IT، درگیری سازمانی در مدیریت و بازبینی به‌کارگیری IT در دستیابی به مجموعه اهداف کلان و عملیاتی سازمان است. ابزار نظام راهبری IT با استاندارد نامحدود کمک می‌کند

که مدیران فنی و غیر فنی و حسابرسان ریسکهای همراه با اطلاعات و مرتبط با توسعه IT را از طریق انجمن نظام راهبری IT و بنیاد کنترل و حسابرسی سیستمهای اطلاعاتی[۵۵] درک کرده و بر اساس چارچوب COBIT آن را مدیریت کنند.

۴- ریسکهای عملیاتی

ریسکهای عملیاتی، بیشتر ناشی از گستره وسیعی از احتمالات بروز خطا و نقصان در عملیات خاص بنگاه تجاری یا مالی هستند. اغلب این ریسک را در مؤسسه‌های مالی و بانکی، ریسکی می‌دانند که به طور مستقیم به ریسکهای اعتباری و بازار مربوط نمی‌شود. این ریسکها حاصل خطای انسانی، رایانه و برنامه‌های آن، خطا در تصمیم‌گیری و حتی زیانهای حاصل از انواع اختلاس هستند. نکته مهم در مورد ریسکهای عملیاتی، پیچیدگی خاص این مفهوم است به گونه‌ای که معمولاً موضوع ریسکهای عملیاتی از موارد دیگر نااطمینانی و خطر پیش روی بنگاه است.

از تعاریفی که برای ریسکهای عملیاتهای در سازمانها ارائه شده‌اند، می‌توان به این موارد اشاره کرد:

- هر گونه ریسکی به جز ریسکهای اعتباری و بازار.
- ریسکهایی که به واسطه انجام عملیات مؤسسه مالی به وجود می‌آیند.

تعریف اول، در حقیقت یک تعریف منفی از ریسک عملیاتی است به این ترتیب که ریسک عملیاتی را به عنوان زیان حاصل از هر نوع فعالیتی غیر از فعالیتهایی که موجب ریسک اعتباری و ریسک بازار می‌شود، در نظر می‌گیرند. این تعریف بسیار گسترده بوده و در بر گیرنده ریسکهای راهبردی[۱] و ریسک شهرت[۲] و نظایر آن می‌شود. در واقع این تعریف غیر از ریسکهای عملیاتی، ریسکهای دیگری را نیز در بر خواهد گرفت که معمولاً جزو ریسکهای عملیاتی محسوب نمی‌شوند.

تعریف دوم نیز تعریف جامعی برای ریسکهای عملیاتی نیست زیرا فقط زیانهای مستقیم حاصل از عملیات سازمان را در بر می‌گیرد، در صورتی که بسیاری از ریسکهای عملیاتی نتیجه غیر مستقیم انجام عملیات سازمان هستند که می‌توان به انواع سرقتها و سوء استفاده‌ها مانند اختلاس اشاره کرد. بنابراین به تعریف جامع‌تر و کاملتری از ریسکهای عملیاتی نیاز داریم، یعنی تعریف استانداردی که کمیته بال برای ریسکهای عملیاتی ارائه داده است.

در حال حاضر بانکهای معتبر جهانی در حال انجام اقدامات قابل توجهی در زمینه مقابله با ریسکهای عملیاتی هستند. این اقدامات در بر گیرنده مراحلی مانند شناسایی ریسکهای عملیاتی در مؤسسه مالی (در اینجا منظور همان زیانهای عملیاتی است)، ارزیابی یا به بیان دقیق‌تر کمی کردن ریسکهای عملیاتی (که نتیجه آن تعیین میزان سرمایه موردنیاز برای مقابله با ریسکهای عملیاتی سازمان است)،

[1]. Strategic Risk

[2]. Reputation Risk

مدیریت ریسکهای عملیاتی که شامل انتقال ریسک (با استفاده از ابزار بیمه و نظایر آن) یا انجام اقداماتی در راستای کاهش میزان ریسکهای عملیاتی است.

بانکهایی که این چالش جدید، یعنی رویارویی با موضوع ریسکهای عملیاتی را می‌پذیرند نیاز به کمکهایی از بیرون سازمان برای شناسایی، ارزیابی و مدیریت ریسکهای عملیاتی خواهند داشت. کمیته بال متعلق به بانک تسویه بین‌الملل، استانداردهایی را در خصوص ریسکهای عملیاتهاتی در سازمانها تدوین کرده و آن را در قالب دستورالعمل‌هایی به بانکهای مختلف سراسر دنیا ابلاغ کرده است، این دستورالعملها در چندین نسخه به روزرسانی شده‌اند و این فرآیند به روزرسانی در آینده نیز ادامه خواهد داشت.

۴-۱- اهمیت ریسکهای عملیاتی

در سالهای اخیر، به دو دلیل توجه زیادی به ریسکهای عملیاتی در سازمانها شده است: نخست، رشد نمایی استفاده از فن‌آوری و دوم، افزایش ارتباطات میان شرکت کنندگان در بازارهای سرمایه. با وجود آنکه فن‌آوری سبب سهولت انجام بسیاری از کارها در سازمان و مهم‌تر از آن رشد بهره‌وری سازمانی شده است اما رشد فن‌آوری، سازمانها را با مسائل و مشکلات جدیدی نیز روبرو کرده است. برای روشن‌تر شدن مطلب، می‌توان به مثال زیر اشاره کرد:

اتوماسیون در سازمانها باعث شده عملیاتی که در گذشته به صورت دستی انجام می‌شد و شاید ساعتها وقت کارکنان اداره صرف انجام آن می‌گردید، هم اکنون در مدت زمان بسیار کوتاه‌تری و با احتمال خطای بسیار کمتری انجام شود، هر چند این رشد فن‌آوری به معنای آن نیست که ریسک حاصل از انجام کارهای اداری کاهش یافته است زیرا در حال حاضر سازمان با ریسک بسیار بزرگتری مانند امکان از کارافتادگی سیستم اتوماسیون روبروست.

ریسک عملیاتی اصولاً مفهوم جدیدی نیست، علت مطرح شدن این بحث در سالهای اخیر، به اهمیت روزافزون آن مربوط می‌شود به طوری که اجتناب از رویارویی با بحث ریسکهای عملیاتی در سازمانها را برای بسیاری از مؤسسه‌های مالی غیر ممکن کرده است.

۵- نتیجه‌گیری

در جاییکه سیستمهای کامپیوتری و اطلاعات تولید شده توسط این فناوری برای پشتیبانی از تصمیم‌گیری وجود دارد، لازم است که قابلیت اطمینان، اعتبار سنجی و کنترلهای داخلی چنین سیستمهایی مورد ارزیابی قرار گیرد. به عبارتی، لازم است که آنها ایمن باشند. چنین فناوری روی آینده هر کسی بدون توجه به حرفه‌اش (وکالت، پزشکی، آموزش، کار اجتماعی، غیره) تأثیر می‌گذارد. به علاوه، حسابرس IT یا متخصص کنترل IT، یکی است و به جلوداری این تغییر و کمک به کارفرما جهت کسب آمادگی مناسب برای مواجهه با محیط کسب و کار در هزاره جدید ادامه خواهد داد. این حرفه پویا، به طور مداوم در حال مواجهه با تغییر و چالشها (محیط یادگیری مستمر) است. با آغاز هزاره جدید فرصت برای شاغلان در این حوزه پر چالش و پویا هرگز بهتر نشده است. پیدایش نظام راهبری IT،

فناوری جدید، کسب و کار الکترونیک و موضوعات قانونی، مرزهایی جدید و ضرورت به‌کارگیری مهارتهای جدید و عقل سلیم را در عملیاتهای کسب و کار جدید مطرح نموده است. درستی کسب و کار، نهاد و شرکت، تحت بررسی مداوم دولت و عموم مردم است. حسابرسی به عنوان فرایندی نهادی می‌تواند بازیگر اصلی در بر پایی مجدد اطمینان عمومی در کسب و کار باشد. در آمریکا، در سایه قانون ساربنز آکسلی، گزارش حسابرسی امروزه ارزش بیشتری نسبت به قبل دارد. همچنانکه، سازمانها برای پردازش و تصمیم‌گیری روزانه بیشتر به حسابرسی فناوری اتکا می‌کنند، در همین راستا، لازمه درگیری حسابرس افزایش خواهد یافت. معرفی حسابرسی فناوری جدید به همراهش ریسکهای جدیدی را می‌آورد. مدیریت به عنوان بخشی از فرایند نظارتی، لازم است اطمینان حاصل کند که ریسکها تحت کنترل کافی هستند. حسابرسان به عنوان بخشی از نظام راهبری IT باید در معرفی فناوری جدید درگیر شوند. به علاوه، مسؤولیت IT از کارکنان IS به کاربران نهایی در حال توزیع شدن است. از اینرو، اطمینان بخشی اطلاعاتی (حسابرسی، کنترل و امنیت) بخش مهمتری از کلیه حسابرسی‌ها خواهند شد.

منابع

۱-ابراهیمی ابراهیم،نقش فناوری اطلاعات در پیشگیری و کشف تقلب،حسابدار،آبان ماه سال ۱۳۹۰،صفحه ۵۶.

۲-ابراهیمی نیوشا،مزیتهای برتر حسابرس فناوری اطلاعات، حسابرس،شماره جلد۵۵،سال ۱۳۹۰،صفحه ۱۰

۳-مهدوی غلامحسین،منصوری شعله،فناوری اطلاعات و تاثیر آن بربهبود کیفیت حسابرسی،حسابرس،شماره جلد۵۱،سال ۱۳۸۹،صفحه ۸۲.

4- American Institute of Certified Public Accountants (AICPA), The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit (SAS 94), 2001.

5- American Institute of Certified Public Accountants (AICPA), Special Committee on Information Assurances, Affect of Information Technology on the Assurance Services Marketplace, 2003.

6- Bierstaker, L. J., Burnaby, P., and Thibodeau, J., The impact of information technology on the audit process: an assessment of the state of the art and implications for the future. Managerial Auditing Journal, Vol 16 (3). pp 159-164, 2001.

7- Caster, P., and Verardo, D., Technology Changes the Form and Competence of Audit Evidence. The CPA Journal. Vol 77 (1). pp 68-70, 2007.

8- Coe, M. J., Trust services: a better way to evaluate I.T. controls: fulfilling the requirements of section 404. Journal of Accountancy 199.3: 69(7), 2005.

9- Chan, S., and Lepeak, S., IT and Sarbanes-Oxley. CMA Management 78.4: 33(4), 2004.

10- Cosserat, G. W., Modern Auditing. John Wiley & Sons`LTD. Second Edition, 2004.

11- Gallegos, F., IT audit career development plan, IS Control Journal, 2, 16-17, 2003.

12- Gallegos, F., IT auditor careers: IT governance provides new roles and opportunities, IS Control Journal, 3, 40-43, 2003.

13- Gallegos, F., Computer forensics: an overview. Information systems audit and control association. Information Systems Control Journal, 6, 2005.

14- Goodwin, B., IT should lead on Sarbanes-Oxley. Computer Weekly 27: p5., 2004.

15- Institute of Internal Auditors (IIA), http://www.theiia.org, 2011.

16- Information Systems Audit and Control Association (ISACA), http://www.isaca.org. 2011.

17- Kruse, W.G., II, and Heiser, J.G. Computer Forensics: Incident Response Essentials, International Journal of Digital Evidence, 2002.

18- Lurie, B. N., Information technology and Sarbanes-Oxley compliance: what the CFO must understand. Bank Accounting and Finance 17.6: 9 (5), 2004.

19- Menkus, B. and Gallegos, F. Introduction to IT Auditing, Auerbach Publishers, Boca Raton, FL., 2002.

20- Piazza, P., IT security requirements of Sarbanes-Oxley. Security Management 40(1), 2004.

21- Senft, S. and Gallegos, F., Information Technology Control and Audit, Auerbach Publications, CRC Press, Third Edition. 2009.

22- Vacca, J.R., Computer Forensics: Computer Crime Scene Investigation, Charles River Media Inc, Hingham, MA., 2002.

23- Wiederkehr, B., IT security programme, IS Control Journal, 3, 30-33, 2003.