ارتباط بین حسابرسی داخلی و امنیت اطلاعات

پروانه خالقی کسبی

از آنجا که فناوری اطلاعات و امنیت اطلاعات نقاط جدایی‌ناپذیر از کنترل‌های داخلی هستند، برای کنترل داخلی چهارچوب یکپارچه‌ای توسط COSO[1] در سال ۱۹۹۷ انتشار یافت که به‌طور خاص، کنترل فناوری اطلاعات را شامل می‌شود. همچنین انجمن حسابرسان داخلی (IIA)[2] و انجمن کنترل و حسابرسی سیستم‌های اطلاعاتی[3] (ISACA)، که هر دو به‌طور مستقیم به چهارچوب‌های COSO مرتبط هستند نیز مشمول این چهارچوب‌ها هستند و این استانداردها شامل روش‌ها و متدهایی اولیه در هر پروسهٔ کنترل برای کمک و راهنمایی در پروسهٔ برنامه‌ریزی‌ها و سیاست‌های فناوری اطلاعات هستند.

امنیت اطلاعات نه تنها برای حفاظت از منابع سازمان، بلکه برای حصول اطمینان از قابلیت اعتماد صورت‌های مالی و دیگر

گزارش‌های مدیریت نیز ضروری است (AICPA and CICA, ۲۰۰۸). در نتیجه COBIT[۴] (چهارچوبی اصولی برای کنترل و راهبری فناوری اطلاعات) تأکید می‌کند که یکی از مسئولیت‌های مدیریت، طراحی و استقرار یک برنامهٔ امنیت اطلاعات اثربخش و مقرون به‌صرفه است (ITGI, ۲۰۰۷).

امروزه کنترل و حسابرسی فناوری اطلاعات (IT)[۵] تبدیل به یک مکانیسم حساس برای تضمین سیستم‌های اطلاعاتی یکپارچه (IS)[۶] و همچنین گزارش‌های مالی سازمان‌ها جهت جلوگیری و ممانعت از وقوع شکست‌های سنگین مالی در آینده از قبیل آنچه در شرکت‌هایی مانند انرون[۷] و ورلدکام[۸] یا بحران‌های مالی جهانی اتفاق افتاد، شده‌اند.

زمانی که شرکتی دارای یک سیاست تدوین شدهٔ روشن و شفّاف از لحاظ قانون است انواع حسابرسی در این ارتباط به صورت زیر انجام می‌شود:

۱. امنیت اطلاعات

۲. پذیرش قوانین و دستورالعمل‌های «PCI: DSS, SOX, HIPAA»

۳. حسابرسی داخلی

چنانچه انجام فرایند حسابرسی داخلی صورت گیرد، این امر منتج به افزایش ارزش داخلی، توسعهٔ چشم‌انداز و اعتبار داخلی سازمان خواهد شد. سازمان‌های پیشرو در بخش خصوصی با استفاده از واحد حسابرسی داخلی آن را به‌عنوان یک زمینهٔ آموزشی در توسعه و انتصاب مدیران آینده مورد توجه قرار می‌دهند زیرا حسابرسی داخلی در عمل جایگاه سهامداران و مدیران اصلی به منظور تصمیم‌سازی در این سازمان‌ها خواهد بود؛ به‌طوری که آنها اقدام به جذب نیروهای متخصص در سطوح بالا پس از بررسی و مشاهدات عملکردی دو تا چهار سالهٔ آنها یا تغییر مسیر شغلی پرسنل حاضر در مدیریت‌های مختلف حسب شناخت از تجارب و توانایی‌های آنها می‌کنند.

امروزه بسیاری از سازمان‌ها و شرکت‌ها در حال تبدیل شدن به سازمان‌هایی با فناوری‌های پیچیده هستند. بر همین اساس با اذعان به اینکه اطلاعات و فناوری اطلاعات، امروزه اهمیت بسیار زیادی برای مدیران دارد، برخی از واحدهای حسابرسی داخلی را بر آن داشته است که نظارت‌های مستمری بر نرم‌افزارهای توسعه‌یافتهٔ تولید اطلاعات در سازمان‌ها به‌صورت لحظه‌ای داشته باشند. این توانایی برای در اختیار داشتن نبض اصلی سازمان‌ها است و به‌عنوان توجه به ارزش‌ها تلقی می‌شود. این فرایند زمانی بهتر خواهد بود که سازمان از لحاظ جغرافیایی دارای پیچیدگی‌های زیادی باشد. همچنین مدل حسابرسی داده‌های اطلاعاتی (EDP) با استفاده از یک گروه کوچک از متخصصین حسابرسی داده‌های اطلاعاتی صورت می‌پذیرد، بر این اساس که واحد حسابرسی داخلی با انجام مصاحبه در بخش‌های در حال توسعه در سازمان، به دنبال افزایش توجه و تخصص در ممیزی و کنترل‌های حسابرسی داده‌های اطلاعاتی است و بیشتر سازمان‌ها همواره به دنبال ادغام عملیات حسابرسی مالی و عملیاتی و حسابرسی داده‌های اطلاعاتی هستند. در شرکت‌ها و سازمان‌هایی که امنیت سیستمهای اطلاعاتی آن ضعیف است، خطر نفوذ به آن سیستم و دستکاری اطلاعات آن زیاد است و خسارت‌های وارده می‌تواند غیرقابل جبران باشد. نیاز به امنیت اطلاعات ایجاب می‌کند که پیش‌بینی‌های لازم توسط مدیریت صورت گیرد تا اطلاعات سیستم از ایمنی مناسبی برخوردار و اطلاعات آن قابل اتکا باشد.

امنیت اطلاعات

در فرهنگ لغت، امنیت به معنی رهایی از خطر، وجود ایمنی، رهایی از ترس یا نگرانی است. واژهٔ «امنیت اطلاعات» به معنی حفاظت از اطلاعات و سیستم‌های اطلاعاتی در مقابل دستیابی و استفادهٔ غیرمجاز از آن است (صفائی، ۱۳۸۳). نتیجهٔ کار و محصول اصلی سیستم‌های کامپیوتری، اطلاعات است. برای یک واحد تجاری، این محصول، اطلاعات

مالی است؛ زیرا اطلاعات مالی نمونه‌ای از محصول تولیدشده به‌وسیلهٔ سیستم اطلاعات حسابداری است. امنیت پردازش معاملات حسابداری، یک موضوع مهم است. از این‌رو، حسابداران به دانش و آگاهی درباره تهدیدات و خطراتی که مربوط به امنیت کامپیوتر می‌شود نیاز دارند (Davis,1997).

نبود امنیت اطلاعات باعث ایجاد نگرانی و دلواپسی عمده برای سازمان‌ها و واحدهای تجاری و غیرتجاری شده است لذا حسابداران و مدیران باید با انواع خطرات و تهدیدات امنیتی به‌منظور حراست و نگهداری از برنامه‌های کاربردی و اطلاعات موجود در کامپیوترهایی که استفاده می‌کنند، آشنا باشند (Daily,2000). بدین منظور حسابداران، حسابرسان و مدیران باید به‌طور صحیح با مهندسان و متخصصان امر درخصوص برقراری امنیت در اطلاعات موجود در سیستم کامپیوتری خود و با انواع متفاوت خطرات و تهدیدهای امنیتی گوناگون مشاوره کنند، زیرا انواع تهدیدها و خطرات برای سیستم اطلاعاتی به موازات پیشرفت سریع فناوری اطلاعات در حال تغییر و تحول است. به‌همین دلیل، حسابرسان همواره تأکید دارند که نیاز برای افزایش امنیت سیستم‌های اطلاعات حسابداری بر طبق آخرین تغییرات و پیشرفت‌های فناوری الزامی است (Davis,1997).

در راستای شناخت و آگاهی از اهمیت راهبری فناوری اطلاعات و چهارچوب راهبری فناوری اطلاعات، اهداف کنترلی برای اطلاعات و فناوری مربوط (COBIT) در ۱۹۹۶ به‌عنوان یک چهارچوب مرجع برای تدوین و مدیریت کنترل‌های داخلی و برقراری سطوح مناسبی از امنیت در فناوری اطلاعات مطرح شد. کوبیت، مجموعه‌ای از اهداف کنترلی پذیرفتهٔ همگانی برای فناوری اطلاعات فراهم می‌کند و به واحدهای تجاری در بیشینه کردن مزایای استفاده از فناوری اطلاعات و تدوین راهبری مناسب اطلاعات و کنترل در سازمان‌ها کمک می‌کند. کوبیت از طریق ارائهٔ چهارچوب و حصول اطمینان از موارد زیر به پشتیبانی از راهبری اطلاعات می‌پردازد:

- هم‌راستا بودن فناوری اطلاعات با اهداف سازمان
- استفاده از منابع فناوری اطلاعات با پذیرش مسئولیت آن
- مدیریت مناسب ریسک‌های فناوری اطل اعات
- توانمندسازی و افزایش مزایای سازمانی به وسیلهٔ فناوری اطلاعات

چهارچوب اهداف کنترلی برای اطلاعات و فناوری مرتبط، موضوع کنترل داخلی را از سه دیدگاه با عناوین اهداف تجاری، منابع فناوری اطلاعات، فرآیندهای فناوری اطلاعات، مورد توجه و بررسی قرار می‌دهد. افزون بر این، اهداف کنترلی برای اطلاعات و فناوری مرتبط در چهار حوزهٔ دانش شامل برنامه‌ریزی

و سازماندهی، تحصیل و اجرا، تحویل و پشتیبانی، کنترل و ارزیابی سازماندهی می‌شوند.

ارتباط حسابرسان داخلی و بخش امنیت سیستم‌های اطلاعاتی

حسابرسان داخلی می‌توانند در برقراری امنیت در سیستم‌های اطلاعات حسابداری نقش مهمی داشته باشند، زیرا آنها به‌طور مستقیم مسئولیت کمک به مدیریت شرکت به‌منظور بهبود کارایی و اثربخشی سازمان را بر عهده دارند. بخشی از این مسئولیت، شامل کمک به طراحی و اجرای سیستم‌های اطلاعات حسابداری است.

در بیشتر سازمان‌ها، هر دو بخش حسابرسی داخلی و سیستم اطلاعاتی با امنیت اطلاعات در تعامل هستند. بخش امنیت اطلاعات، مسئولیت اصلی طراحی، استقرار و حفظ برنامهٔ ایمنی اثربخش و مقرون به‌صرفهٔ اطلاعات را بر عهده دارد و حسابرسی داخلی بررسی و تجزیه و تحلیل مستقل از عملکرد امنیت اطلاعات سازمان، ارائه می‌کند. در حالت ایده‌آل بازخورد ارائه شده توسط حسابرسی داخلی می‌تواند برای ارتقای اثربخشی کلی امنیت اطلاعات سازمان کاربرد داشته باشد. این دو بخش می‌بایست به‌صورت هم‌افزا با یکدیگر کار کنند تا اثربخشی برنامهٔ امنیت سیستم اطلاعاتی سازمان را به حدّ اعلی برسانند. والاس[9] و همکارانش(۲۰۱۱) شواهدی ارائه کردند که سطح مشارکت بین بخش‌های حسابرسی داخلی و امنیت اطلاعات دارای ارتباط مثبتی با سطح تطابق سازمان با الزامات کنترل داخلی مرتبط با فناوری اطلاعات تصریح شده در قانون ساربنز آکسلی(SOX) بود.

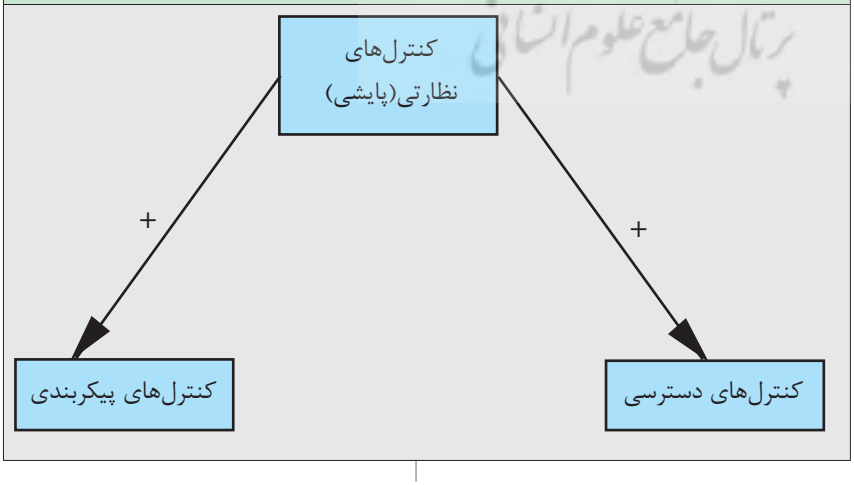
کنگرهٔ آمریکا در واکنش به رسوایی شرکت‌ها در اواخر سدهٔ بیستم، قانون ساربنز- آکسلی را در ۲۰۰۲ تصویب کرد. این قانون جامع‌ترین قانون مرتبط با حسابداری سازمان‌های حرفه‌ای است. روش‌های ساربنز-آکسلی، قانونی فراگیر و به‌طور وسیعی رویه‌های تجاری شرکت‌ها را مانند قوانین مدیریت ارشد، هیأت مدیره، حسابرسان مستقل و کمیتهٔ حسابرسی تغییر داده است. بخش ۴۰۴ قانون ساربنز- آکسلی با عنوان «ارزیابی مدیریت از کنترل‌های داخلی» است که بر اهمیت سامانه‌های کنترل داخلی مناسب به‌عنوان بخشی از حفظ و نگهداری اعتمادپذیری و یکپارچگی سامانه‌های اطلاعاتی حسابداری تأکید دارد. سازمان‌های رعایت‌کنندهٔ قانون ساربنز – آکسلی در بخشی از گزارش‌های سالانهٔ خود باید دامنه و کفایت کنترل‌های داخلی را بیاورند.

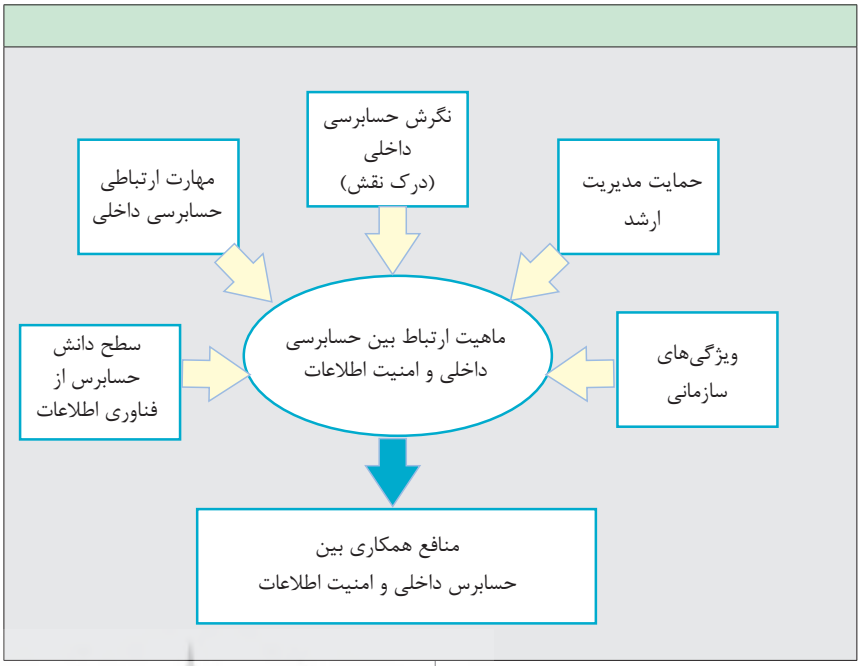
حسابرسان داخلی باید به اجرای بررسی‌های فناوری اطلاعات یا کنترل‌های امنیتی سایبری و همچنین انطباق با رویه‌های امنیتی توجه کنند. رویهٔ امنیت شبکه می‌تواند فنی و پیچیده باشد، بنابراین حسابرسان داخلی با آموزش تخصصی و فنی محدود و بررسی محدود ضمنی ایمنی سایبری نمی‌توانند به صورت کارا عمل کنند. حسابرسان داخلی دارای مهارت‌های فنی، می‌توانند در برنامه‌ریزی و اجرای حسابرسی مفید واقع شوند. آنها باید سطح درک خود را از کنترل‌ها و خطرات موضوعات مهم رشد دهند. به دلیل وجود جهان به هم پیوسته، بنگاه‌های اقتصادی به ایجاد و گسترش کنترل‌های ایمنی سایبری مؤثر و قوی نیاز دارند (Moeller , ۲۰۰۹).

نقش حسابرسان داخلی در حسابرسی فناوری اطلاعات، ارائهٔ تضمین کافی و مناسب کنترل‌ها است. اولین نقش حسابرسی به جز در زمینه‌های خدمات مشاورهٔ مدیریت، اطمینان از این است که آیا کنترل‌های داخلی در محل‌های مناسب و قابل اطمینان تعریف شده و اجرایی‌هستند یا خیر و اینکه اجزای آنها دارای شیوه‌ای کارآمد و مؤثر است. بنابراین، درحالی که مدیریت، نقش اطمینان‌بخش را دارد حسابرسان داخلی نقش بیمه‌کننده را داراهستند.

سازمان‌ها برای فراهم کردن سطحی مطلوب از امنیت اطلاعات، مجموعه‌ای از ابزارها و رویه‌های متفاوت را به‌کار می‌برند. حسابداران و حسابرسان معمولاً کنترل‌ها

شکل ۱: ارتباط میان انواع مختلف کنترل‌های امنیت اطلاعات (۲۰۰۹)





را به پیشگیرانه، کشف‌کننده یا اصلاح کننده طبقه‌بندی می‌کنند(Ratliff, ۱۹۹۶). کنترل‌های دسترسی شامل ابزارهایی مانند فایروال، سیستم پیشگیری از نفوذ، کنترل دسترسی فیزیکی و روش‌های مجاز و معتبر هستند که برای کاهش احتمال وقوع حوادث نامطلوب در دستیابی غیر مجاز به سیستم به کار می‌روند. کنترل‌های نظارتی نیز شامل مستندسازی و تجزیه و تحلیل فعالیت روزانه است که برای کشف مشکلات و ارائهٔ اطلاعات ضروری برای اصلاح آنها به کار برده می‌شوند.

مطابق با تحقیق رانزبتم و میترا[۱۰]، سه نوع کنترل امنیت سیستم اطلاعاتی دارای اهداف متفاوتی هستند. کنترل‌های پیکربندی مستقیماً احتمال خطر شناسایی امنیت اطلاعات را با قفل کردن تلاش‌های اکتشافی هدفمندانه کاهش می‌دهد. همچنین کنترل‌های دسترسی به‌طور مستقیم خطر در معرض کشف قرار گرفتن را به‌وسیلهٔ قفل کردن تلاش‌های غیرمجاز برای دسترسی به سیستم کاهش می‌دهد. برخلاف دو نوع کنترل قبلی، کنترل‌های نظارتی به‌طور غیر مستقیم خطر یک رویداد را به‌وسیلهٔ ارتقای اثربخشی دو گروه کنترل دیگر کاهش می‌دهد. برای مثال، مستندسازی مناسب ریسک غفلت از سیستم اصلی را هنگام تغییر تنظیمات پیش‌فرض، به‌کارگیری قطعات، استقرار فایروال‌ها و اجرای دیگر انواع کنترل‌های امنیتی کاهش می‌دهد. به‌طور مشابه، تجزیه و تحلیل فعالیت روزانه می‌تواند به شناسایی دلایل وقایع کمک کند، چنین دانشی می‌تواند برای تعدیل کنترل‌های موجود به منظور کاهش ریسک بروز مشکلات مشابه در آینده، استفاده شود. رانزبتم و میترا بر نقش واحد امنیت سیستم اطلاعاتی در پیادهسازی هر سه نوع کنترلها تمرکز داشتند. با این وجود، به عنوان یک راهنمای اصولی COBIT، پیشنهاد می‌کنند که واحد حسابرسی داخلی سازمان باید به‌طور دوره‌ای اثربخشی کنترل‌های داخلی شامل کنترل‌های مرتبط با امنیت سیستم اطلاعاتی را ارزیابی کند، بنابراین گسترش نقش حسابرسی داخلی می‌تواند اثربخشی تلاش در بخش امنیت اطلاعات سازمان را ارتقا بخشد.

بازخورد حسابرسی داخلی می‌تواند اثربخشی و کارایی فرایند امنیت اطلاعات را با توسعهٔ مسئولیت اشخاص برای عملکرد امنیتی اقدامات اصلاحی در واکنش به یافته‌ها و توصیه‌های حسابرسی بهبود بخشد. تمایل مدیران بخش امنیت اطلاعات در پاسخگویی به گزارش‌های حسابرس داخلی براساس کیفیت ارتباط آنها با بخش حسابرسی داخلی تعیین می‌شود. اگرچه ارتباطی خوب بین بخش‌های حسابرسی داخلی و امنیت اطلاعات با بهبود سطح توافق یک سازمان با الزامات کنترل داخلی مرتبط با فناوری اطلاعات از قانون SOX پیدا شده است، اما شواهد نشان می‌دهند که ارتباط بین بخش حسابرسی داخلی و سایر بخش‌های یک سازمان اغلب تغییر شکل یافته است. بنابراین، این موضوع برای درک عواملی که ماهیت ارتباط بین بخش‌های امنیت اطلاعات و حسابرسی داخلی را تحت تأثیر قرار می‌دهد، مهم است.

ارتباط نادرست یا ناکافی بین حسابرسی داخلی و امنیت اطلاعات می‌تواند اثری منفی بر ارتباط بین دو بخش مزبور بگذارد؛ در حقیقت شواهد قابل ملاحظه‌ای وجود دارد که مشکلات ارتباطی و واکنش‌های متفاوت در سابقه و دانش، زیربنای عدم توافق‌هایی بوده است که اغلب میان مدیران مالی و مدیران فناوری اطلاعات رخ داده است. تفاوت موجود در اندازه، فرهنگ، منبع و روش‌های مدیریتی هر یک از این دو بخش دیگر علت‌های بالقوه در ایجاد مشکل بین واحدهای یک سازمان هستند. نهایتاً تفاوت در دسترسی

به مدیریت ارشد نیز می‌تواند ارتباط بین حسابرسی داخلی و امنیت اطلاعات را متأثر کند. عموماً حسابرسی داخلی از نظر کارکردی به هیأت مدیره و از نظر اداری به مدیریت ارشد گزارش می‌کند. در مقابل بخش ایمنی اطلاعات اغلب گزارشگری مستقیم به مدیریت ارشد ندارد امّا به مدیر فناوری اطلاعات گزارش می‌کند. بنابراین ممکن است بین دو بخش حسابرسی داخلی و امنیت سیستم اطلاعاتی ارتباط غیربهینه وجود داشته باشد و ویژگی‌های انجام کار در سازمان از نظر کیفیت ارتباطات تأثیر پذیرد.

اثر ویژگی‌های حسابرسان داخلی بر ارتباطات بین کارکنان حسابرسان داخلی و امنیت اطلاعات

ویژگی‌های حسابرس، ماهیت ارتباط بین بخش‌های حسابرسی داخلی و امنیت اطلاعات را متأثر می‌کند و شامل عواملی نظیر سطح دانش فنی حسابرسان، مهارت‌های ارتباطی و درک نقش حسابرس داخلی در مقابل امنیت اطلاعات است. سطح دانش حسابرس از فناوری اطلاعات و مهارت‌های ارتباطی به‌خصوص وضوح و شفافیت، اثر ویژه‌ای بر ماهیت ارتباط بین دو بخش دارد. یک حسابرس داخلی فناوری اطلاعات، باید قادر به تشریح دامنه کنترل‌ها و چرایی آنها پیش از آزمون باشد زیرا این توانایی باعث پذیرش کنترل‌ها توسط بخش فناوری اطلاعات می‌شود و زمانی که حسابرس داخلی نقش خود را، به جای پلیس سازمان، ارائهٔ خدمات مشاوره‌ای می‌داند؛ اطمینان مشترک بین بخش‌های حسابرسی داخلی و امنیت اطلاعات پدید می‌آید و در نتیجه افزایش اعتماد مشارکت و همکاری نیز افزایش می‌یابد.

منافع همکاری بین حسابرسی داخلی و امنیت اطلاعات

سطح دانش فناوری اطلاعات بخش حسابرسی داخلی کیفیت ارتباط بین حسابرسی داخلی و امنیت اطلاعات را متأثر می‌کند سطوح بالاتر دانش فنی اطلاعات منتج به ارتباط موثرتر و عمیق‌تر بین دو بخش می‌شود.

مهارت‌های ارتباطی بین حسابرسی داخلی به‌طور مستقیم بر سطح همکاری بین حسابرسی داخلی و امنیت اطلاعات اثر دارد. تعریف شفاف دامنه و هدف یک کار حسابرسی منجر به افزایش اطمینان بخش امنیت سیستم اطلاعاتی و همکاری بیشتر آن می‌شود.

نگرش حسابرسی داخلی، مستقیماً بر سطح همکاری حسابرسی داخلی و امنیت اطلاعات اثر می‌گذارد. زمانی که حسابرسی داخلی یک نگرش مشارکتی یا بهبود فرایند داشته باشد سطح بالاتری از اطمینان و همکاری بین حسابرسی داخلی و امنیت اطلاعات وجود خواهد داشت، زمانی که حسابرسی داخلی یک نگرش پلیسی نسبت به کار داشته باشد همکاری کمتری وجود خواهد داشت.

سطح بالای تشویق توسط مدیریت ارشد برای بخش‌های حسابرسی داخلی و امنیت اطلاعات به همکاری متقابل طراحی شده است. اثرگذاری مدیریت ارشد بر ماهیت ارتباط بین کارکنان حسابرسی داخلی و امنیت اطلاعات مخصوصاً زمانی که

حسابرسان ارشد و افراد اجرایی در بخش امنیت یک نگرش مشارکتی داشته باشند منجر به همکاری بیشتر آنها و پاسخگویی مسئولان اجرایی برای هر بخش می‌شود. ارتباط منسجم بین بخش‌های امنیت سیستم اطلاعاتی و حسابرسی داخلی انطباق کاربران را با رویه‌ها و سیاست‌های امنیت اطلاعات سازمان افزایش می‌دهد و همچنین اثربخشی حسابرسی داخلی را به‌وسیلهٔ توجه مستقیم به حوزه‌های دارای ریسک بیشتر بهبود می‌دهد.

حسابرسی داخلی یکی از ارکان مهم راهبری در یک سازمان است که با اتکا به آن صاحبان سازمان از اثربخشی و کارایی فعالیت‌های سازمان اطمینان حاصل می‌کنند. امروزه استفاده از فناوری اطلاعات برای کلیه سازمان‌های بزرگ امری ضروری و اجتناب‌ناپذیر است چرا که با گسترش فعالیت‌ها و تغییرات سریع تکنولوژی، لازم است که سازمان‌ها از انعطاف‌پذیری لازم برخوردار باشند و این امر محقق نمی‌شود مگر در سایهٔ استفاده از فناوری اطلاعات. از این رو استقرار چهارچوب حاکمیت فناوری اطلاعات در سازمان‌ها قبل از هر کاری باید مورد حسابرسی قرار گیرد تا از هدر رفتن منابع سازمان جلوگیری شود. بدیهی است هر چقدر ابعاد سازمان، بزرگتر باشد، الزام استقرار چهارچوب حاکمیت فناوری اطلاعات اهمیت بیشتری پیدا می‌کند.

نظارت، یک قسمت جداناشدنی از کنترل داخلی اثربخش است (کوزو، ۲۰۰۴). بنابراین، نظارت منظم کنترل امنیت اطلاعات می‌تواند اثربخشی کلی برنامهٔ امنیت اطلاعاتی سازمان را ارتقا دهد. اگرچه نظارت بر کنترل امنیت اطلاعات می‌تواند وجود داشته باشد و معمولاً هست امّا انجام آن توسط بخش امنیت اطلاعات، اگر با استفاده از نتایج بررسی حسابرسی داخلی همراه شود، منافع بیشتری به بار خواهد آورد. با این حال منافع بازخورد مستقل به سطح دانش حسابرسان داخلی از فناوری اطلاعات، نگرش آنها به همکاری با کارکنان بخش امنیت اطلاعات (نقش پلیس در مقابل مشاور امین)، حمایت مدیریت از همکاری بین حسابرسی داخلی و امنیت اطلاعات و خصوصیات سازمانی مانند الزامات انطباق با مقررات و کانال‌های ارتباطی رسمی بستگی دارد. ■

پی‌نوشت‌ها:

1-Committee of Sponsoring Organizations of the Treadway Commission
2- Institute of Internal Auditors
3- Information Systems Audit and Control Association
4- Control objective for Information and Related Technology
5- Information Technology
6- Information Systems
7- Enron
8- WorldCom
9- Wallace
10- Ransbotham and Mitra

منابع:

صفائی، احمد، امنیت شبکه، انتشارات دانش‌پرور، چاپ اول ۱۳۸۳

AICPA, CICA. Trust services principles and criteria. American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants; 2008.

Bodin LD, Gordon LA, Loeb MP. Information security and risk management. Commun ACM 2008;51:64–8.

Bussey J. Has time come for more CIOs to start reporting to the top? Wall St J 2011. May 17, accessed via http://online.wsj.com/article/SB10001424052748704281504576327510720752684.html.

COSO. Enterprise risk management — integrated framework: executive summary; 2004.

Daily, C. and Lueblfing, M., Defending the Security of the Accounting System, the CPA Journal, Oct . 2000, pp. 62،65

D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf Syst Res 2009;20:79–98.

Davis, C. E., An Assessment of Accounting Information Security, CPA Journal, March, 1997 :28،35

Dhillon G, Tejay G, Hong W. Identifying governance dimensions to evaluate information systems security in organizations.

Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Q 2010;34:549–66.

Kumar RL, Park S, Subramaniam C. Understanding the value of countermeasure portfolios in information security. J Manag Inf Syst 2008;25:241–79.

Moeller, Robert. (2009) Seventh Edition. John Wiley & Sons, Inc. Brink's Modern Internal Auditing.

Paul John Steinbart, Robyn L. Raschke, Graham Gal, William N. Dilla, 2012, The relationship between internal audit and information security: An exploratory investigation, International Journal of Accounting Information Systems 13 (2012) 228–243

Phelps D, Milne K. Leveraging IT controls to improve IT operating performance. The Institute of Internal Auditors Research Foundation; 2008.

Ransbotham S, Mitra S. Choice and chance: a conceptual model of paths to information security compromise. Inf Syst Res 2009;20:121–39.

Ratliff RL, Wallace WA, Sumners GE, McFarland WG, Loebbecke JK. Internal auditing: principles and techniques. 2nd edition.Altamonte Springs: Institute of Internal Auditors; 1996.

Proceedings of the 40th Hawaii International Conference on Systems Sciences; 2007.

Dittenhofer MA, Ramamoorti S, Ziegenfuss DE, Evans RL. Behavioral dimensions of internal auditing: a practical guide to professional relationships in internal auditing. The Institute of Internal Auditors Research Foundation; 2010.

Europe Research Services CFO. Are CFOs from Mars and CIOs from Venus? Overcoming the perception gap to enhance the finance-IT relationship. London: CFO Publishing Corporation; 2008

Hawkey K, Muldner K, Beznosov K. Searching for the right fit: balancing IT security management model trade-offs. IEEE Internet Comput 2008:22–30.

IIA. Global technology audit guide 1: information technology controls. Altamonte Springs, FL: Institute of Internal Auditors; 2005.

IIA. Practice advisory 1110-1. Organizational independence. Altamonte Springs, FL: Institute of Internal Auditors; 2009.

IIA. International Standards for the Professional Practice of Internal Auditing. Attribute Standard 1100—Independence and Objectivity; 2011.

ITGI. COBIT 4.1: control objectives for information and related technology. Rolling Meadows, IL: IT Governance Institute; 2007.

پروانه خالقی کسبی: دکتری حسابداری- حسابدار رسمی