مطالعات اقتصاد، مدیریت مالی و حسابداری

دوره ۲، شماره ۲/۲، تابستان ۱۳۹۵

صفحات ۷۹- ۸۸

ISSN: ۲٤۷٦-٤٤۳٤

www.irijournals.com

ارتباط بین حسابرسی داخلی و امنیت اطلاعات؛ تحقیق اکتشافی

عسگر پاک‌مرام [۱]، ابراهیم رستم نژاد [۲]، داریوش قهرمانی [۳]

[۱] استادیار حسابداری دانشگاه آزاد اسلامی واحد بناب، ایران

[۲] دانشجوی کارشناسی ارشد حسابداری دانشگاه آزاد اسلامی واحد بناب، ایران

[۳] کارشناس ارشد مدیریت دولتی

چکیده

واحدهای حسابرسی داخلی و ایمنی اطلاعات در یک سازمان، می بایست به صورت هم افزا با یکدیگر کار کنند؛ کارکنان بخش ایمنی اطلاعات به طراحی، استقرار و عملیاتی کردن روش ها و فناوری های مختلف به منظور حمایت از منابع اطلاعاتی سازمان می پردازند. از سوی دیگر حسابرسی داخلی با ارائه‌ی بازخوردهای دوره ای در خصوص اثربخشی آن فعالیت ها، پیشنهاداتی برای بهبود آن ها مطرح می نمایند. با این وجود گزارشات موجود در ادبیات حرفه بیانگر آن است که دو بخش مزبور همواره دارای ارتباط هماهنگ با یکدیگر نیستند. این مقاله، نخستین بخش از یک پروژه ی تحقیقاتی طراحی شده برای بررسی ماهیت ارتباط بین ۲ بخش حسابرسی داخلی و ایمنی اطلاعات است. در ادامه، نتایج یک سری مصاحبه های نیمه ساختار یافته با افراد شاغل در بخش های حسابرسی داخلی و ایمنی اطلاعات را گزارش خواهیم کرد. در این پژوهش با ایجاد یک مدل اکتشافی از عوامل موثر بر ماهیت ارتباط بین بخش های حسابرسی داخلی و ایمنی اطلاعات، منافع بالقوه ای که سازمان ها می توانند از این ارتباط بدست آورند را توصیف کرده و همچنین پیشنهاداتی برای تحقیقات آتی ارائه کنیم.

واژه‌های کلیدی: حسابرسی داخلی، امنیت سیستم اطلاعاتی، رفتارهای ایمنی.

۱- مقدمه

توجه به تأثیر تغییرات و عوامل محیطی و افزایش اطلاع‌رسانی و استقبال سازمان‌ها در استفاده از خدمات حسابرسی داخلی در کنار گزارش‌های حسابداری مدیریت، شناسایی رابطه‌ی عملکرد حسابرسی داخلی و اهمیت آن بر کاربرد ابزارهای حسابداری مدیریت ضرورت دارد. صلاحیت حرفه‌ای به عنوان یکی از مشخصه‌های منحصر به فرد حسابرسی داخلی در مقایسه با سایر خصوصیات حسابرسان داخلی (تضاد منافع، استقلال و درستکاری و بی‌طرفی) برکاربرد ابزارهای حسابداری مدیریت تأثیر بیشتری دارد (حاجیها و حقیقی، ۱۳۹۵).

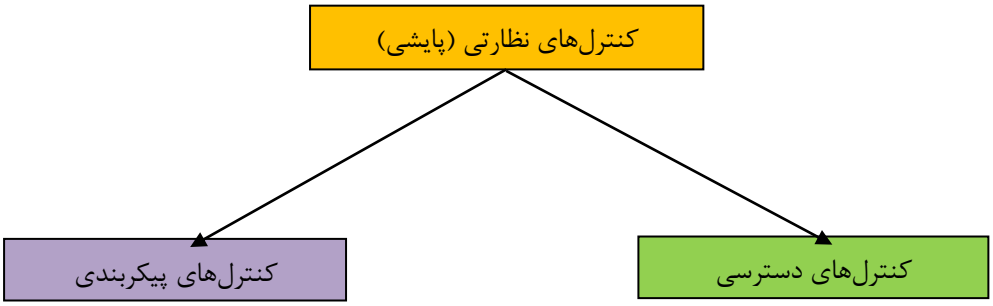
امنیت اطلاعات نه تنها برای حفاظت از منابع سازمان، بلکه برای حصول اطمینان از قابلیت اعتماد صورتهای مالی و دیگر گزارشات مدیریت نیز ضروری است (AICPA and CICA،2008). در نتیجه COBIT (یک چارچوب هنجاری برای کنترل و راهبری فناوری اطلاعات) تأکید می کند (ITGI،2007)، که یکی از مسئولیتهای مدیریت، طراحی و استقرار یک برنامه ی ایمنی اطلاعات اثربخش و مقرون به صرفه است. لذا، محققان این حوزه شروع به بررسی ابعاد و زوایای راهبری ایمنی اطلاعات کرده اند. جریان اول تحقیقات بر اندازه گیری ارزش سرمایه گذاری ها در ایمنی اطلاعات، تمرکز کرده اند (گوردون و لوئب، ۲۰۰۵؛ کومار و همکاران، ۲۰۰۸). جریان دوم تحقیقات به آزمون واکنش های بازار سهام به افشاهای ایمنی اطلاعات موسسات (گوردون و همکاران، ۲۰۱۰) و رویدادها (ایتو و همکاران، ۲۰۱۰) پرداخته اند. جریان سوم تحقیقات نیز بر آزمون کردن روش سیاست های ایمنی اطلاعات سازمان ها برای ارتقای رضایت مصرف کننده ی نهایی معطوف شده اند (دارسی و همکاران، ۲۰۰۹؛ اسپیرز و بارکی،۲۰۱۰).

با این وجود، به جنبه های عملیاتی راهبری ایمنی اطلاعات، توجه کمی شده است (دیلن و همکاران، ۲۰۰۷). در واقع، در بررسیهای انجام شده در تحقیقات قبلی پیرامون راهبری ایمنی سیستم اطلاعاتی، نتیجه گیری شده است (دیلن و میشرا، ۲۰۰۶) که نقش انسان ها و موضوعات مرتبط با مدیریت مردم در سازمان ها، مورد تأکید تعاریف عمومی از راهبری ایمنی سیستم اطلاعاتی نیست (فلپس و میلن، ۲۰۰۸). این تحقیقات به طور خاص متذکر شدند که دید ISCG(راهبری ایمنی سیستم اطلاعاتی) جاری، اجازه ی ورود اهمیت فرایند حسابرسی سیستمها و مدیریت جزئیات ایمنی در سطح عملیاتی فرایند کسب و کار را نمی دهد. علاوه بر این، یک پیمایش که اخیراً توسط IIA(انجمن حسابرسان داخلی) انجام شده است، توصیه می کند که یک رویکرد تضامنی بین عملیات حسابرسی داخلی و فناوری اطلاعات وجود داشته باشد و هدف این رویکرد را بهبود بازده کسب شده از سرمایه گذاری در فعالیت های کنترلی راهبری اطلاعات می داند. به طور کلی فقدان توجه به ابعاد عملیاتی راهبری ایمنی اطلاعات و مخصوصاً ارتباط بین بخش های حسابرسی داخلی و ایمنی اطلاعات به طور حیرت آوری موجب تأکید بر ادبیات دستوری در این موضوع شده است. برای مثال COBIT تجویز می کند که مدیریت باید یک ساختار مربوط، دارای ارتباط بهینه و هماهنگ بین بخش فناوری اطلاعات و ... گروه مطلوب شرکت، ایجاد و حفظ نماید. علاوه بر آن کنترل محیطی باید بر مبنای یک فرهنگی باشد که... مشارکت بین بخش ها و کار گروهی را تشویق نماید. از این گذشته، برای بدست آوردن اطمینان مستقل (داخلی و خارجی) درباره ی هم جهت بودن فناوری اطلاعات با ... سیاستها، استانداردها و روش های سازمان اهمیت دارد.

در بیشتر سازمان ها، هر دو بخش حسابرسی داخلی و سیستم اطلاعاتی با ایمنی اطلاعات در تعامل هستند. بخش ایمنی اطلاعات، مسئولیت اصلی طراحی، استقرار و حفظ برنامه ایمنی اثربخش و مقرون به صرفه‌ی اطلاعات را بر عهده دارد. حسابرسی داخلی یک بررسی و تحلیل مستقل از کارهای ایمنی اطلاعات سازمان، ارائه می کند. در حالت ایده آل بازخورد ارائه شده توسط حسابرسی داخلی می تواند برای ارتقای اثربخشی کلی ایمنی اطلاعات سازمان کاربرد داشته باشد. این ۲ بخش می بایست به صورت هم افزا با یکدیگر کار کنند تا اثر بخشی برنامه‌ی ایمنی سیستم اطلاعاتی سازمان را به حد عالی برسانند. در واقع، (والاس و همکارانش،۲۰۱۱) شواهدی ارائه کردند که سطح مشارکت بین بخش های حسابرسی داخلی و ایمنی اطلاعات دارای ارتباط مثبتی با سطح تطابق سازمان با الزامات کنترل داخلی مرتبط با فناوری اطلاعات تصریح شده در قانون ساربنز آکسلی (SOX) بود.

با وجود اهمیت و ارزشی که می تواند از رابطه ی بین حسابرسی داخلی و ایمنی اطلاعات حاصل شود، هیچ گونه تحقیق تجربی که در آن چگونگی عمل متقابل در ۲ بخش بررسی شده باشد، وجود ندارد. این مقاله، نتایج نخستین مطالعه ی صورت گرفته برای برداشتن اولین گام جهت پرکردن این فاصله در ادبیات موضوع را گزارش می کند. در این پژوهش یک سری مصاحبه ی نیمه ساختاریافته با شاغلان هر ۲ بخش حسابرسی داخلی و ایمنی سیستم اطلاعاتی به منظور شناسایی عوامل تعیین کننده ماهیت ارتباط بین ۲ بخش تهیه گردیده است. ضعف و کمبود در تحقیقات پیشین، استفاده از یک رویکرد اکتشافی مانند مطالعه ی موردی و مصاحبه‌های نیمه ساختار یافته را مناسب می سازد. اعمال این روش‌ها در سازمان‌های متعدد، فرصتی برای اکتشاف زیربنای موضوع تحقیق و ارائه‌ی پیشنهاد برای تحقیقات و بررسی‌های آتی فراهم می‌آورد (یین، ۲۰۰۳).

ادامه ی این تحقیق به شکل زیر سازماندهی شده است؛ بخش ۲ به مرور ادبیات پیشین پرداخته و مدلی ارائه خواهد داد که در آن چگونگی کار ۲ بخش حسابرسی داخلی و ایمنی اطلاعات با یکدیگر برای کمک به سازمان در دستیابی به سطحی اثربخش و مقرون به صرفه از امنیت اطلاعات، ارائه شده است. بخش ۳ روش مصاحبه ی ساختاریافته و سوابق مصاحبه شونده ها و سازمان های متبوعه ی آن ها را تشریح می کند. بخش ۴ مطالب عمومی استخراج شده از مصاحبه ها را ارائه می نماید. در بخش ۵ نیز با ایجاد یک مدل از عوامل موثر بر ارتباط بین بخش های حسابرسی داخلی و ایمنی اطلاعات به نتیجه گیری از تحقیق پرداخته و مجموعه ای از پیشنهادات را بیان می‌نماید که می توان از آن ها به عنوان راهنما برای تحقیقات آتی درباره‌ی این موضوع استفاده نمود.



شکل ۱: ارتباط میان انواع مختلف کنترل های ایمنی اطلاعات (منبع: رانسبتهام و میترا، ۲۰۰۹)

۲- ادبیات تحقیق

برای آزمون عوامل موثر بر ماهیت ارتباط بین بخش‌های حسابرسی داخلی و ایمنی اطلاعات یک سازمان، یک مجموعه مصاحبه ساختار یافته با ۴ سازمان فعال در بخش آموزشی ترتیب تهیه گردیده است. پیوست A لیستی از پرسش‌ها و محرک‌ها و منابع زیربنایی برای طرح هر موضوع را نشان می‌دهد.

به ۴ دلیل بر موسسات بخش آموزشی تمرکز گردیده است، نخست آن‌که ارتباط بین امنیت اطلاعات و حسابرسی داخلی را در یک بخش نوعی (معمولی) به جای یک بخشی که بهترین رویه‌های مدرن و به روز را به کار می‌برد، کشف گردد. بنابراین صنایعی مانند بخش دفاعی و یا موسسات خدمات مالی انتخاب نگردید. دوم آن‌که، بخش آموزشی مصرف‌کننده‌های متنوعی برحسب هر دوی کارکنان (دانشکده و پرسنل) و مشتریان (دانشجویان) که استفاده زیادی از کاربردهای کاربر واحد آموزشی می‌نمایند. بنابراین بخش آموزشی باید مجموعه‌ی پیچیده‌ای از چالش‌های ایمنی اطلاعات که از دسترسی به شبکه‌ی موسسه برای افرادی به جز کارمندان به وجود می‌آید را ارزیابی کند. با این وجود یک مجموعه کارمند (دانشکده) یک منفعت خاصی به گروه کاربر نشان می‌دهند به خاطر درجه‌ی بالای خود مختاری و استقلال آنان. دلیل سوم آن‌که، بخش آموزش باید با یک تعداد الزامات و مقررات متفاوتی تطابق داشته باشد. همه‌ی این موضوعات در ارتباط با بخش خصوصی در قانون حق آموزش خانواده و امنیت، مشخص شده است. آن مقررات همچنین موضوع محدودیت‌های قانون GLBA برای پردازش معاملات مالی

و تطابق بیشتر با استاندارد PCI-DSS برای تراکنش‌های کارت اعتباری نیز است. در نهایت، موسسات آموزشی به طور پیوسته تغییرات مرتبط با فرایند کسب و کارشان را پیگیری می‌کنند. برای مثال به عنوان یک فناوری آموزشی، موسسات باید ایمنی اطلاعات مرتبط با محتوای ارائه شده در دوره‌های آموزشی و گزارشات محرمانه‌ی دانشجویان به صورت برخط را حفظ نمایند. همه‌ی این عوامل بخش آموزشی را به عنوان نقطه‌ی آغازین برای بررسی ماهیت ارتباط بین واحدهای حسابرسی داخلی و ایمنی اطلاعات مطرح می‌سازد.

مصاحبه‌ها در محل کار مصاحبه شونده‌ها برگزار شد. ۲ عضو گروه تحقیقاتی در هر مصاحبه شرکت داشتند. در موسسات A و B و D مصاحبه با شخص مذبور را انجام داد و دیگری از طریق کنفرانس تلفنی مشارکت داشت. در موسسه C، هر دو عضو گروه تحقیقاتی به طور حضوری برای مصاحبه رفتند. مصاحبه‌های صورت گرفته در ۳ موسسه A و B و C برای هر دو بخش و در موسسه D تنها با مصاحبه شونده‌ی شاغل در بخش ایمنی اطلاعات ارائه شده است، زیرا در موسسه D واحد حسابرسی داخلی برون‌سپاری شده بود.

لیست پرسش های پیوست A ساختاری برای مصاحبه ها فراهم می‌کرد، اما به مصاحبه شونده اجازه داده شده بود تا درباره موضوعات و مباحثی که فکر می‌کردند مهم است صحبت کنند. هر مصاحبه بین ۴۵ تا۹۰ دقیقه به طول انجامید و آنها پس از ضبط برای تحلیل های بعدی نوشته شدند. مشارکت کننده‌گان مطلع بودند که هدف مطالعه درک بهتر ارتباط بین امنیت فناوری اطلاعات و حسابرسی داخلی است.

مطالعه به صورت اکتشافی با هدف شناسایی الگو های جاری تهیه گردید، بنابراین از رویکرد کیفی با کدبندی توصیف شده توسط میلز و هوبرما (۱۹۹۴) استفاده شد آنها ایجاد یک ماتریس برای تحلیل داده ها را پیشنهاد کرده بودند زیرا آن یک روش خلاصه و در عین حال قاعده مند است که به درک مفهوم و معنی پایگاه داده‌ها را کمک می‌کند.

۳- پیشینه پژوهشی

سازمان‌ها برای فراهم کردن سطح مطلوب از ایمنی اطلاعات، مجموعه ای از ابزارها و رویه های متفاوت را به کار می برند. حسابداران و حسابرسان معمولاً کنترل ها را به پیشگیرانه، کشف کننده یا اصلاح کننده طبقه بندی می کنند (راتلیف، ۱۹۹۶). که احتمال موفقیت حمله‌کنندگان در شناسایی ضعف‌ها را کاهش می‌دهد. کنترل‌های دسترسی شامل ابزارهای مانند دیوار آتش، سیستم پیشگیری از حمله، کنترل دسترسی فیزیکی و روش‌های مجاز و معتبر هستند که برای کاهش احتمال موفقیت حمله‌کنندگان در دستیابی غیر مجاز به سیستم به کار می‌رود. کنترل‌های نظارتی شامل مستندسازی و تحلیل فعالیت روزانه است که بخش برای کشف مشکلات و ارائه اطلاعات ضروری برای پیشگیری آن‌ها به کار می‌برد.

مطابق با تحقیق راشبوتا و میترا (۲۰۰۹)، سه نوع کنترل ایمنی سیستم اطلاعاتی دارای اهداف متفاوتی هستند. کنترهای پیکربندی مستقیما احتمال در خطر کشف گرفتن ایمنی اطلاعات را با قفل کردن تلاش‌های اکتشافی هدفمندانه کاهش می-دهد. همچنین کنترل‌های دسترسی به طور مستقیم خطر در معرض کشف قرار گرفتن را بوسیله قفل کردن تلاش‌های غیر مجاز برای دسترسی به سیستم کاهش می‌دهد. برخلاف دو نوع کنترل قبلی، کنترل‌های نظارتی به طور غیر مستقیم خطر یک رویداد را بوسیله‌ی ارتقای اثربخشی دو گروه کنترل دیگر کاهش می‌دهد. برای مثال، مستندسازی مناسب ریسک چشم‌پوشی از سیستم اصلی را زمانی که پیکربندی‌های معین جایگزین، تعمیرات به کار گرفته شده، دیوار آتش کسترش یافته و استقرار دیگر انواع کنترل‌های ایمنی را کاهش می‌دهد. به طور مشابه، تحلیل فعالیت روزانه می‌تواند به شناسایی دلایل رویدادها کمک کند، مانند دانش که می‌تواند استفاده شود برای تعدیل کنترل‌های موجود برای کاهش ریسک که یک حمله مشابه در آینده موفق شود.

راشبوتام و میترا (۲۰۰۹)، بر نقش واحد ایمنی سیستم اطلاعاتی در پیاده‌سازی هر سه نوع کنترل‌ها تمرکز داشتند. با این وجود، به عنوان یک راهنمای هنجاریCOBIT، پیشنهاد می‌کند که واحد حسابرسی داخل سازمان باید به طور دوره‌ای اثربخشی کنترل‌های داخلی شامل کنترل‌های مرتبط با ایمنی سیستم اطلاعاتی را ارزیابی کند. بنابراین و با تاکید منطقی

راشبوتام و میترا (۲۰۰۹) بر ارزش کنترل‌های نظارتی پیشنهاد می‌کند گسترش بررسی حسابرسی داخلی می‌تواند اثربخشی تلاش ایمنی اطلاعات سازمان را ارتقاء بخشد.

با این وجود، راشبوتام و میترا (۲۰۰۹)، ارزش کنترل‌های نظارتی در ارتقای اثربخشی دیگر روش‌های ایمنی اطلاعات را آزمون نکرد بلکه فقط ارزش بالقوه آن را بدیهی پنداشتند. همچنین، مدل آن‌ها به طور ضمنی وجود یک فرایند بازخورد که از اطلاعات گردآوری شده توسط کنترل‌های نظارتی برای تعدیل و بهبود کنترل‌های دسترسی و پیکربندی سازمان استفاده می-کند را فرض می‌کند. بازخورد حسابرسی داخلی می‌تواند اثربخشی و کارایی فرایند ایمنی اطلاعات را تنها با توسعه‌ی مسئولیت اشخاص برای اقدامات اصلاح بخش ایمنی اطلاعات در پاسخگویی به هر گزارش حسابرسی تعیین شود. حداقل در این بخش، برای کیفیت ارتباط آن‌ها با بخش حسابرسی داخلی دارد. اگر چه یک ارتباط خوب بین بخش‌های حسابرسی داخلی و ایمنی اطلاعات با بهبود سطح توافق یک سازمان با الزامات کنترل داخلی مرتبط با فناوری اطلاعات از قانون SOX پیدا شده است، اما همچنین شواهد نشان می‌دهند که ارتباط بین بخش حسلبرسی داخلی و سایر بخش‌های یک سازمان اغلب تغییر شکل یافته است. بنابراین، این موضوع برای درک عواملی که ماهیت ارتباط بین بخش‌های ایمنی اطلاعات و حسابرسی داخلی را متاثر می‌کند، مهم است.

ارتباط ضعیف بین حسابرسی داخلی و ایمنی اطلاعات می‌تواند یک اثر منفی روی ارتباط بین این واحدها داشته باشد. در واقع شواهد قابل ملاحظه‌ای وجود دارد که مشکلات ارتباطی تفاوت‌های بین پیشینه و دانش زیربنای بیشتر عدم توافق‌ها که اغلب بین مدیر مالی و مدیر فناوری اطلاعات رخ می‌دهد، انعکاس می‌یابد. تفاوت‌ها در اندازه بخش، فرهنگ، منابع و نگرش مدیریت واحد دیگر دلایل... مشکلات ارتباطی بین واحدهای سازمان هستند. در نهایت، تفاوت در دسترسی به مدیریت ارشد می‌تواند بر ارتباط بین دو بخش اثر گذارد.

ارتباط نادرست یا ناکافی بین حسابرسی داخلی و ایمنی اطلاعات می تواند اثری منفی بر ارتباط بین ۲ بخش مزبور بگذارد، در حقیقت شواهد قابل ملاحظه ای وجود دارد که مشکلات ارتباطی که 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 آنکه تفاوت در دسترسی به مدریت ارشد نیز می تواند ارتباط بین حسابرسی داخلی و ایمنی اطلاعات را متاثر کند. عموماً حسابرسی داخلی از نظر کارکردی به هیات مدیره و از نظر اداری به مدیریت ارشد گزارش می کند. در مقابل بخش ایمنی اطلاعات اغلب گزارشگری مستقیم به مدیریت ارشد ندارد اما معمولاً به به مدیر فناوری اطلاعات گزارش می کند.

بنابرین، بین دو بخش حسابرسی داخلی و ایمنی سیستم اطلاعاتی، ممکن است دارای ارتباط غیر بهینه باشند و ممکن است ویژگی‌های انجام کار در سازمان از نظر کیفیت ارتباطات تاثیر پذیرد. به منظور کشف این احتمال و شناسایی دیگر عوامل بالقوه که مانع ایجاد همکاری بهینه بین دو بخش مزبور شود و یا مانع پیشرفت روابط آنها می‌شود، در ادامه یک مجموعه مصاحبه نیمه ساختار یافته با حسابرسان داخلی و افراد شاغل در ایمنی سیستم اطلاعاتی تدوین گردیده است.

۴- یافته های مصاحبه

۴-۱-اثر ویژگیهای حسابرسان داخلی بر ارتباطات بین کارکنان حسابرسان داخلی و ایمنی اطلاعات

مصاحبه شونده ها مشخص کردند که ویژگیهای حسابرس، ماهیت ارتباط بین بخش‌های حسابرسی داخلی و ایمنی اطلاعات را متاثر می‌کند.عوامل خاصی که توسط آنان اشاره شده بود شامل سطح دانش فنی حسابرسان، مهارت‌های ارتباطی و درک نقش حسابرس داخلی در مقابل ایمنی اطلاعات بود.

الف)اهمیت دانش فنی حسابرسان

کارکنان هر دو بخش حسابرسی داخلی و ایمنی اطلاعات تصدیق کردند که سطح دانش حسابرس از فناوری اطلاعات، اثر ویژه ای بر ماهیت ارتباط بین ۲ بخش دارد.

ب)مهارتهای ارتباطی

مهارت‌های ارتباطی به خصوص وضوح و شفافیت، توسط مصاحبه شونده ها مهم شمرده شده است. برای نمونه حسابرس داخلی موسسه Aبیان کرد:

یک حسابرس فناوری فناوری اطلاعات خوب باید قادر به تشریح دامنه کنترل‌ها و چرایی آنها پیش از آزمون باشد، در ۹۹درصد پرس و جوهای محقق نشان داد این توانایی باعث پذیرش کنترل‌ها توسط بخش فناوری اطلاعات می شود.

ج) طرز برخورد حسابرس و ادراک نقش حسابرسی

به طور خلاصه، زمانی که حسابرس داخلی نقش خود را، بیشتر به جای پلیس، مشاوره ای می داند؛ اطمینان مشترک بین بخش های حسابرسی داخلی و ایمنی اطلاعات پدیدآمده و در نتیجه ی افزایش اعتماد مشارکت و همکاری نیز افزایش می یابد.

۴-۲-اثر مدیریت ارشد بر ارتباط بین حسابرسی داخلی و ایمنی اطلاعات

سُطح الزام مدیریت ارشد برای امنیت به عنوان یک عامل مهم در اثر بخشی کلی ایمنی اطلاعات سازمان، بیان شده است. در نهایت در هر یک از مصاحبه‌ها مصاحبه شوندگان (حسابرسان داخلی وکارکنان بخش ایمنی اطلاعات) توسط مدیریت ارشد حمایت می شدند؛ با این وجود معیارهای ردیابی شده در شاغلان ایمنی اطلاعات ۳ موسسه غیرانتفاعی A,B,D مشخص ساخت که علی رغم اینکه مدیریت ارشد اصولاً حمایت زیادی از ایمنی اطلاعات کرده است اما منابع مناسبی برای نیازهای ضروری ایمنی اطلاعات اختصاص نداده است. به دلیل بالا بودن میزان آزادی بیان و استقلال دانشکده‌ها، واقعاً همنوایی مناسبی با سطح اجرایی مدیریت دانشکده وجود داشت. آنها گزارشات مستقیمی برای نظارت متمرکز بر فرایند کسب وکار دریافت کرده اند. در طول ۲سال گروها به خوبی ریسک‌ها را متوجه شده اند. مدیر ایمنی اطلاعات موسسه A "علاوه بر این در موسسه B حسابرس داخلی مشخص ساخت که توانایی مدیریت ارشد برای ارائه منابع کافی، دلیل عدم دستیابی به دانش فنی عمیق درباره ایمنی سیستم اطلاعاتی بوده است در مقابل در موسسهC ؛ هم مدیر ایمنی سیستم اطلاعاتی وهم حسابرس داخلی فکر می کنند که مدیریت ارشد موسسه بودجه کافی برای ایمنی اطلاعات را فراهم کرده است.علاوه بر آن مزایای مشخصی برای ایمنی اطلاعات مانند مواردی که مدیر ایمنی اطلاعات مشخص ساخته، ارائه کرده اند. برای دستیابی به یک چیزی که آنها جزو اهداف سالانه می دانند، تعداد زیادی مزایای وابسته به دستیابی و بر اورده ساختن حسابرسی در تطابق با نقایص یافته های اصلی ایجاد کرده اند.

برای ضمانت اجرایی داشتن قانون ساربنزآکسلی میتوان مشوق هایی از سوی مدیریت نسبت به اهداف عمومی و مخصوصاً موضوعات مرتبط با ایمنی اطلاعات اختصاص داد او همچنین خاطر نشان ساخت که قانون ساربنزآکسلی بر نگرش مدیریت ارشد از بابت تمرکز بر ایجاد و درک نقش ایمنی اطلاعات بر عملیات پشتیبانی سازمان اثر داشته است راشبوتام و میترا (۲۰۰۹).

به طور خلاصه، اگرچه در تحقیق انجام شده، افراد شاغل در هر ۲ بخش موسسات مورد مصاحبه، مدیریت ارشد را حامی ایمنی اطلاعات پنداشته شد، اما در اصل فقط در موسسات انتفاعی توافق برای مدیریت ارشد در قبال منابع قابل اندازه گیری و پاداش متناسب با آن وجود دارد. در نتیجه انتظار می رود که به دنبال پیگیری منافع شخصی خود در افزایش ارزش سازمان و مشارکت در ایمنی اطلاعات باشند.

۴-۳-پیامدهای ارتباط بین حسابرسی داخلی و ایمنی اطلاعات

موارد مطرح شده توسط مصاحبه های شونده موسسات A وC یک ارتباط صمیمی بین بخشهای حسابرسی داخلی وایمنی اطلاعات ارائه کردند که میتواند ُبرای سازمان مفید باشد از دیدگاه ایمنی اطلاعات پشتیبانی حسابرسی داخلی میتواند به پیاده سازی قدرتمند روشهای ایمنی وبهبود کارایی آنها کمک کند. مدیر فناوری اطلاعات موسسهA بیان کرد که ما یک ارتباط متقابل و مثبت داریم، منفعت واقعاً زیادی به ما در دستیابی به اهدافمان از دیدگاه ایمنی اطلاعات میرسد وما اهمیت تغییرات کنترل‌ها را درک میکنیم، در مجموع نکات مطرح شده در مصاحبه ها نشان دادند که حسابرسی داخلی به طور بالقوه میتواند از

چندین راه ارزش افزایی کند؛ همانطور که انتظار می‌رود که بازخورد حسابرسی داخلی بتواند فرصت های بهبود اثر بخشی تمام انواع کنترل‌های سیستم اطلاعاتی را شناسایی کند برای مثال نتایج حسابرسی ایمنی اطلاعات می‌تواند نشان دهد که سطح واقعی انطباق کاربر نهایی با سیاست‌ها تا چه میزان است. انجام یک کار حسابرسی داخلی همچنین، به موقع بودن اقدامات اطلاعاتی از فعالیت‌های روزانه ایمنی و دیگر سیستم‌های نظارتی را ارزیابی می‌کند. در نهایت حسابرسی داخلی می‌تواند میزان اقدامات اصلاحی مانند درصد دستگاهای پیکربندی که در پاسخ به پویش‌های داوطلبانه تعدیل شده‌اند را شناسایی کند پیامدهای مرتبط با سطوح متفاوت همکاری بین بخش‌های حسابرسی داخلی و ایمنی اطلاعات یک موضوع مهم برای تحقیقات آتی هستند. از دیدگاه حسابرسی داخلی یک ارتباط خوب با بخش ایمنی اطلاعات برای بهبود مدیریت ریسک ادراک شده است حسابرس داخلی موسسه A بیان می‌کند که من تمام کارکنان ایمنی اطلاعات دانشکده و برخی از کارکنان پشتیبانی آنها را می شناسم، این ارتباط از طریق اطمینان بخشی با حسابرسی فناوری اطلاعات و تمرکز بر حوزه ها وحساب‌های پر ریسک موجب ارزش افزایی به سازمان می‌شود.

۵- بحث و خلاصه

اطلاعات تجربی کمی درباره‌ی ماهیت ارتباط بین حسابرسی داخلی و ایمنی اطلاعات وجود دارد. برای شروع بررسی‌ها در این زمینه، یک مجموعه مصاحبه نیمه ساختار یافته با شاغلان در هر ۲ بخش صورت داده شد، شواهدی از ماهیت متفاوت ارتباط بین دو بخش در ۴ موسسه مورد مصاحبه یافت گردید. در موسسه A و C یک ارتباط قوی بین ۲ بخش به چشم خورد که کاملاً ارتباط مثبت و دارای منافع برای هر دو بخش بود. در مقابل در ۲ بخش D و B یک ارتباط محدود بین ۲ بخش به نظر رسید و مصاحبه کنندگان به منفعت خاصی که از همکاری ۲ بخش پدیدآمده باشد اشاره نکردند.

تحلیل گفته‌های مصاحبه شونده‌ها، چندین حوزه بالقوه که بازخورد حسابرسی داخلی می‌تواند برای ارتقای جنبه‌های متفاوت ایمنی اطلاعات به کار رود، را شناسایی کرد. یک موضوع مهم برای تحقیقات آتی تمرکز بر چگونگی شناسایی منافع است مطالعه اکتشافی بیان می کند که شناسایی آن منافع احتمالاً به چیزی فراتر از ماهیت ارتباط بین ۲ بخش بستگی دارد. شکل ۲ یک مدل از عوامل ارائه گردیده و تعدادی پیشنهاد ابتدایی که می‌تواند در تحقیقات بعدی بررسی شود را ارائه گردیده، ۳پیشنهاد نخست از واکنش مصاحبه شونده‌ها در هر ۴ موسسه به پرسش درباره چگونگی اثر گذاری ویژگی‌های حسابرسان داخلی بر کیفیت ارتباط بین ۲بخش حسابرسی داخلی وایمنی اطلاعات مطرح می شوند.

پیشنهاد ۱

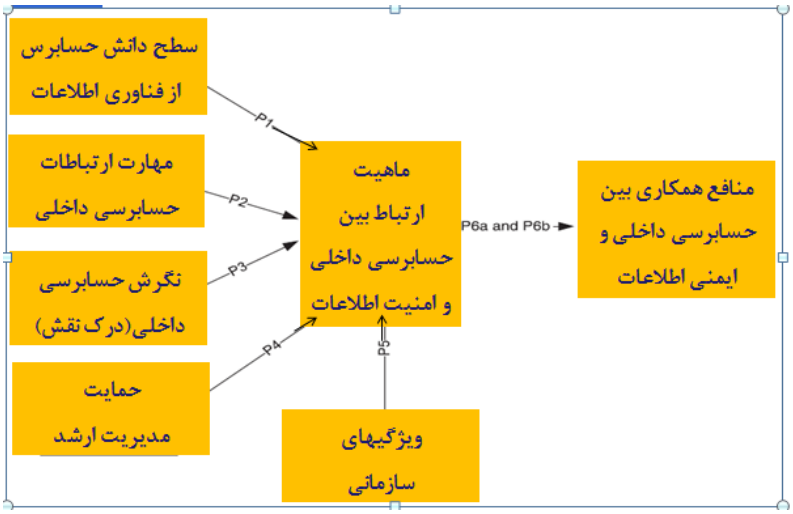
سطح دانش فناوری اطلاعات بخش حسابرسی داخلی کیفیت ارتباط بین حسابرسی داخلی و ایمنی اطلاعات را متاثر می‌کند سطوح بالاتر دانش فنی اطلاعات منتج به ارتباط موثرتر و عمیق‌تر بین دو بخش می‌شود.

پیشنهاد ۲

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

پیشنهاد۳

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



جدول۲- ارائه جدولی برای پیشنهادات، منبع یافته‌های پژوهش

پیشنهاد ۴

بر مبنای گفته‌های مصاحبه شوندگان در موسسه C اظهار می‌داشتند سطح بالای تشویق توسط مدیریت ارشد برای بخش‌های حسابرسی داخلی وایمنی اطلاعات به همکاری متقابل طراحی شده است.

پیشنهاد ۵ : اثر گذاری مدیریت ارشد بر ماهیت ارتباط بین کارکنان حسابرسی داخلی و ایمنی اطلاعات مخصوصاً زمانی که حسابرسان ارشد وافراد اجرایی در بخش ایمنی یک نگرش مشارکتی داشته باشند منجر به همکاری بیشتر آنها و پاسخگویی مسئولان اجرایی برای هر بخش می‌شود.

پیشنهاد ۵

شواهد مصاحبه های انجام شده که عمق ارتباط بین بخش‌های ایمنی سیستم اطلاعاتی و حسابرسی داخلی در موسسه C که هدف آن کسب سود بوده است وانتفاعی بود را در ارتباط با موضوع قانون ساربنزآکسلی نسبت به سه موسسه بررسی شده دیگر که به طور مستقیم موضوع ساربنزآکسلی نبودند را انعکاس می‌دهد. همچنین این واقعیت بیان می‌کند که عمق ارتباط بین بخش‌های حسابرسی داخلی و ایمنی سیستم اطلاعاتی در موسسه B که حسابرسی داخلی به طور مستقیم به شورای نمایندگان گزارش می‌داد، کانال رسمی برای ارتباط بخش سیستم اطلاعاتی نداشته قوی نبود.

ویژگی‌های سازمانی مانند ماهیت الزامات انطباق با مقررات وکانال‌های ارتباط سازمانی ماهیت ارتباط بین بخش‌های حسابرسی داخلی و ایمنی سیستم اطلاعا تی را متاثر کند. نتایج مصاحبه‌های ما برخی شاخص‌های ابتدایی را ارائه کرد که حسابرسی داخلی می‌تواندعلاو بر ارتباط مثبت با ایمنی اطلاعات نیز مفید باشد این نکات در قالب دو پیشنهاد ۶ الف و۶ ب طرح می شود.

پیشنهاد ۶ الف: یک ارتباط همکارانه بین بخش‌های ایمنی سیستم اطلاعاتی و حسابرسی داخلی انطباق کاربران با رویه‌ها و سیاست‌های امنیت اطلاعات سازمان را افزایش می دهد.

پیشنهاد ۶ب: یک ارتباط همکارانه بین دو بخش حسابرسی داخلی و ایمنی سیستم اطلاعاتی اثر بخشی حسابرسی داخلی را بوسیله توجه مستقیم به حوزه های دارای ریسک بیشتر بهبود می‌دهد اگر چه مصاحبه شونده‌ها در موسسات A و C یک تعداد منافع برای ارتباط دوستانه و صمیمی بین بخشهای حسابرسی داخلی و ایمنی سیستم اطلاعاتی مطرح کردند، اما حسابرسی داخلی به حفظ استقلال و بی طرفی خود برای انجام کار به طور اثر بخشی نیاز دارد.

۶- بحث و نتیجه‌گیری

نظارت (پایش) یک جزء جداناشدنی از کنترل داخلی اثربخش است (کوزو،۲۰۰۴)، بنابراین، نظارت منظم کنترل ایمنی اطلاعات می‌تواند اثربخشی کلی برنامه‌ی ایمنی اطلاعات سازمان را ارتقا دهد (رانسبتهام و میترا، ۲۰۰۹). اگرچه نظارت بر کنترل ایمنی اطلاعات می تواند وجود داشته باشد و معمولاً هست، اما انجام آن توسط بخش ایمنی اطلاعات، منافع بیشتری به بار خواهد آورد اگر با استفاده از نتایج بررسی حسابرسی داخلی همراه شود (والاس و همکاران، ۲۰۱۱). البته نتایج این تحقیق اظهار می دارد که منافع بازخورد مستقل به سطح دانش حسابرسان داخلی از فناوری اطلاعات، نگرش آنها به همکاری با کارکنان بخش ایمنی اطلاعات (نقش پلیس در مقابل مشاور امین)، حمایت مدیریت از همکاری بین حسابرسی داخلی و ایمنی اطلاعات، و خصوصیات سازمانی مانند الزامات انطباق با مقررات و کانال های ارتباطی رسمی بستگی دارد.

منابع

۱. حاجیها، زهره. حقیقی، حسین.(۱۳۹۵). بررسی رابطه‌ی کاربرد ابزارهای حسابداری مدیریت بر صلاحیت حرفه‌ای حسابرسان داخلی در شرکت‌های تولیدی بورس اوراق بهادار تهران. فصلنامه دانش حسابداری و حسابرسی مدیریت. پاییز۱۳۹۵. سال پنجم. ش ۱۹. ص ۴۷-۶۰.

2. AICPA, CICA. Trust services principles and criteria. American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants; 2008.
3. Bodin LD, Gordon LA, Loeb MP. Evaluating information security investments using the analytical hierarchy process. Commun ACM 2005;48:79–83.
4. Bodin LD, Gordon LA, Loeb MP. Information security and risk management. Commun ACM 2008;51:64–8.
5. COSO. Enterprise risk management — integrated framework: executive summary; 2004.
6. 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.
7. Dhillon G, Tejay G, Hong W. Identifying governance dimensions to evaluate information systems security in organizations. Proceedings of the 40th Hawaii International Conference on Systems Sciences; 2007.
8. IIA. International Standards for the Professional Practice of Internal Auditing. Attribute Standard 1100—Independence and Objectivity; 2011.
9. ITGI. COBIT 4.1: control objectives for information and related technology. Rolling Meadows, IL: IT Governance Institute; 2007.
10. Ito K, Kagaya T, Kim H. Information security governance to enhance corporate value. NRI Secure Technologies; 2010.
11. Kumar RL, Park S, Subramaniam C. Understanding the value of countermeasure portfolios in information security. J Manag Inf Syst 2008;25:241–79.
12. Mishra S, Dhillon G. Information systems security governance research: a behavioral perspective in 1st Annual symposium on information assurance. Academic Track of 9th Annual NYS Cyber Security Conference, New York, USA; 2006. p. 18–26.
13. Phelps D, Milne K. Leveraging IT controls to improve IT operating performance. The Institute of Internal Auditors Research Foundation; 2008.
14. Ransbotham S, Mitra S. Choice and chance: a conceptual model of paths to information security compromise. Inf Syst Res 2009;20:121–39.

15. Ratliff RL, Wallace WA, Sumners GE, McFarland WG, Loebbecke JK. Internal auditing: principles and techniques. 2nd edition. Altamonte Springs: Institute of Internal Auditors; 1996.
16. Spears JL, Barki H. User participation in information systems security risk management. MIS Q 2010;34:503–22.
17. Wallace L, Lin H, Cefaratti MA. Information security and Sarbanes–Oxley compliance: an exploratory study. J Inf Syst 2011;25:185–212.
18. Yin RK. Case study research design and methods (3rd ed). Thousand Oaks: Sage; 2003.