

بررسی تاثیر رابطه خوب بین حسابرسي داخلي و امنيت اطلاعات بر پيامدهای امنيت اطلاعات در بين بانکهای پذيرفته شده در بورس اوراق بهادار تهران

مریم رحمانی

کارشناس ارشد رشته حسابرسي، دانشگاه آزاد اسلامي واحد نور

نام نویسنده مسئول:

مریم رحمانی

تاریخ دریافت: ۱۳۹۹/۱۲/۲

تاریخ پذیرش: ۱۴۰۰/۲/۱۵

چکیده

در سال های اخیر، امنيت اطلاعات به عنوان یکی از نگرانی های عمده برای متخصصان حسابداری در نظر گرفته شده است. حسابرسي داخلي و امنيت اطلاعات هر دو از ابزارهای حیاتی مدیریت سازمان، جهت رسیدن به اهداف سازمان می باشند. از این رو، در این تحقیق به بررسی تأثیر ساختار گزارشگری امنيت اطلاعات و حمایت مدیران ارشد بر اثربخشی امنيت اطلاعات، با توجه به کیفیت رابطه امنيت اطلاعات و حسابرسي داخلي، پرداخته شده است. روش این تحقیق، بر اساس هدف، کاربردی و بر اساس نحوه گردآوری داده ها، توصیفی-پیمایشی و از نوع همبستگی می باشد. جامعه آماری مورد مطالعه این تحقیق، شامل کلیه کارکنان واحدهای حسابرسي داخلي و امنيت اطلاعات سازمان های مرکزی بانک های پذیرفته شده در بورس اوراق بهادار تهران، در نظر گرفته شده است. با توجه به اینکه، حجم تقریبی جامعه، ۳۶۰ نفر در نظر گرفته شده است، حجم نمونه، از طریق فرمول کوکران، ۱۸۶ نفر، تعیین شد که با استفاده از روش نمونه گیری غیرتصادفی در دسترس، انتخاب شدند. ابزار جمع آوری اطلاعات در این تحقیق پرسشنامه می باشد که روایی محتوایی آن، مورد تأیید قرار گرفته است و پایایی آن، با محاسبه آلفای کرونباخ، تأیید شده است. در این مطالعه به منظور تحلیل داده ها از دو رویکرد کلی آماری آمار توصیفی و آمار استنباطی استفاده گردید. روش حداقل مربعات جزئی با نرم افزار Smart PLS در آمار استنباطی، به منظور بررسی معناداری فرضیه ها، مورد استفاده قرار گرفت. نتایج آزمون هفت فرضیه این تحقیق، حاکی از این بود که؛ ساختار گزارشگری امنيت اطلاعات، بر اثربخشی امنيت اطلاعات، تأثیر مثبت و معناداری دارد. همچنین نتایج نشان داد که؛ سطح حمایت مدیریت ارشد از امنيت اطلاعات، بر اثربخشی امنيت اطلاعات و کیفیت رابطه این واحد با حسابرسي داخلي، تأثیر مثبت و معناداری دارد. همچنین با توجه به اینکه، کیفیت رابطه امنيت اطلاعات با حسابرسي داخلي، بر اثربخشی امنيت اطلاعات، مؤثر است، می توان این عامل را میانجی گر تأثیر سطح حمایت مدیریت ارشد بر اثربخشی امنيت اطلاعات دانست.

واژگان کلیدی: ساختار گزارشگری، حمایت مدیریت ارشد، امنيت اطلاعات، حسابرسي داخلي، اثربخشی.

مقدمه

با نفوذ سیستم‌های اطلاعاتی آنلاین به اغلب مشاغل، امنیت اطلاعات اهمیت خاصی در سازمان‌ها و به ویژه در حسابرسی داخلی یافته است. حسابرسی داخلی و امنیت اطلاعات هر دو از ابزارهای حیاتی مدیریت سازمان، جهت رسیدن به اهداف سازمان می‌باشند (اشتاینبارت^۱ و همکاران، ۲۰۱۸). از این رو در این تحقیق به بررسی تاثیر رابطه خوب بین حسابرسی داخلی و امنیت اطلاعات بر پیامدهای امنیت اطلاعات در بین بانکهای پذیرفته شده در بورس اوراق بهادار تهران پرداخته شده است. جرایم اینترنتی می‌تواند یک تاثیر اقتصادی مستقیم و معنادار روی سازمان از طریق غرامت دارایی، سرقت اطلاعات محرمانه حساس، اختلال در فعالیت‌های آنلاین و هزینه‌های حقوقی برای حل و فصل مطالبات مصرف‌کنندگان آسیب‌دیده، داشته باشد (هنگ^۲، ۲۰۱۶). همچنین این مقوله می‌تواند اثر اقتصادی غیرمستقیم داشته باشد، زیرا افشای عواملی چون ریسک بالای امنیت اطلاعات و نقض امنیت اطلاعات می‌تواند به طور قابل توجهی بر ارزش شرکت تاثیر بگذارد (هیگز^۳ و همکاران، ۲۰۱۶). علاوه بر این امنیت اطلاعات سازمان، یک نقطه کانونی متفاوت از نگرانی و یک موضوع ریسک متفاوت است، زیرا عاملان آن اغلب ناشناخته و خارج از سازمان هستند. این موضوع، در مقایسه با سرقت دارایی و خطرات افشای مالی است که در آن تمرکز اغلب بر اقدامات افراد قابل شناسایی درون سازمان است. اکنون این سوال مطرح می‌گردد که چه کسانی در سازمان مسئول مدیریت ریسک امنیت اطلاعات می‌باشند؟ به نظر می‌رسد که پاسخ منطقی این باشد که یک گروه تخصصی مرتبط با عملکرد امنیت اطلاعات مسئول مدیریت ریسک امنیت اطلاعات می‌باشند. با این حال گزارش‌های انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی (ISACA)^۴ در سال ۲۰۱۱ نشان می‌دهد که مدیریت ریسک امنیت اطلاعات نه تنها بر عهده کمیته تخصصی امنیت اطلاعات است، بلکه گروه‌های دیگر در سازمان از جمله کمیته حسابرسی داخلی (IAF)^۵ نیز مسئول آن می‌باشند. از این رو، در سال‌های اخیر، امنیت اطلاعات به عنوان یکی از نگرانی‌های عمده برای متخصصان حسابداری در نظر گرفته شده است و مسئله مدیریت ریسک امنیت اطلاعات یک زمینه مهم را برای تحقیق در مورد حسابرسی داخلی به عنوان یک ابزار حاکمیت شرکتی و مدیریت ریسک فراهم کرده است (هیل^۶، ۲۰۱۵). با این وجود به جنبه‌های عملیاتی راهبری امنیت اطلاعات توسط کمیته حسابرسی داخلی توجه کمی شده است. در همین راستا مسئله اصلی تحقیق حاضر بررسی این است که برقراری ارتباط متقابل و بهینه بین کمیته حسابرسی داخلی و کمیته امنیت اطلاعات چه تاثیری بر نتایج امنیت اطلاعات دارد. در بیشتر سازمان‌ها هر دو بخش حسابرسی داخلی و امنیت اطلاعات در تعامل هستند. بخش امنیت اطلاعات، مسئولیت اصلی طراحی، استقرار و حفظ برنامه ایمنی اثربخش و مقرون به صرفه اطلاعات را بر عهده دارد. حسابرسی داخلی نیز یک بررسی و تحلیل مستقل از کارهای امنیت اطلاعات سازمان ارائه می‌کند. در حالت ایده‌آل بازخورد ارائه شده توسط حسابرسی داخلی می‌تواند برای ارتقاء اثربخشی کلی امنیت اطلاعات سازمان کاربرد داشته باشد. این دو بخش می‌بایست به صورت هم‌افزا با یکدیگر کار کنند تا اثربخشی برنامه امنیت سیستم‌های اطلاعاتی سازمان را به حد عالی برسانند (هاولکا و مرهوت^۷، ۲۰۱۳). در همین زمینه والاس^۸ و همکاران (۲۰۱۱) شواهدی ارائه کرده‌اند 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^۹ ساربنز آکسلی (SOX)^{۱۰} بود. لذا با توجه به این پشتوانه نظری و با عنایت به این موضوع که گسترش روزافزون واحدهای اقتصادی، توسعه فناوری ارتباطات و ریسک‌های مرتبط با آن، نیازهای نظارتی را به وجود آورده

است و این شرایط موجب اهمیت یافتن کنترل‌های داخلی شده است، تحقیق حاضر مبتنی بر مطالعه اشتاینبارت و همکاران (۲۰۱۸) جنبه‌هایی از اثرات کیفیت ارتباط بین کمیته‌های حسابرسی داخلی و امنیت اطلاعات را مورد بررسی قرار داده است. در واقع این تحقیق بررسی می‌کند که آیا کمیته حسابرسی داخلی و ارتباط آن با کمیته امنیت اطلاعات می‌تواند نقش با اهمیتی در برقراری و بهبود امنیت اطلاعات سازمان برقرار سازد یا خیر؟ دغدغه پژوهشگر از طرح چنین موضوعی علاوه بر کمبود شواهد تجربی در زمینه این نظریه، در حالت کلی چالش‌های پیش‌روی حسابرسی داخلی در ایران شامل نبود استانداردهای حسابرسی داخلی مدون شده، استقرار نیافتن نظام حاکمیت شرکتی در بسیاری از شرکت‌ها و به تبع آن نبود اهداف و راهبردهای تجاری و عملیاتی و نبود دستورالعمل‌های مناسب اجرای کار می‌باشد که فرآیند حسابرسی داخلی و وظایف و مسئولیت‌های آن را در حوزه‌های مختلف از جمله کنترل و نظارت بر امنیت اطلاعات، بدون برنامه و عدم درک علمی و عملی و با مشکل مواجه ساخته است. با توجه به این مطالب سوال اصلی پژوهش این‌گونه مطرح می‌گردد:

رابطه خوب بین حسابرسی داخلی و امنیت اطلاعات چه تاثیری بر پیامدهای امنیت اطلاعات در بانک‌های پذیرفته شده در بورس اوراق بهادار دارد؟

مبانی نظری و پیشینه پژوهش

سیستم‌های اطلاعاتی

سیستم اطلاعات به جمع‌آوری، پردازش، ذخیره، تحلیل و انتشار اطلاعات برای یک هدف خاص می‌پردازد. سیستم اطلاعات مانند هر سیستم دیگری دارای ورودی و خروجی است. این سیستم با استفاده از فناوری‌هایی مانند کامپیوتر، ورودی‌ها را پردازش کرده، خروجی‌ها را از طریق شبکه‌های الکترونیکی به کاربران یا سیستم‌های دیگر می‌فرستد (آقایی و همکاران، ۱۳۹۵). چهار کاربرد اصلی سیستم‌های اطلاعاتی عبارتند از: مدیریت مالی و حسابداری، کنترل مواد و موجودی، دریافت و تحقق سفارش، اتوماسیون نیروی فروش (حقیقی نسب و تقوی، ۱۳۹۱). اطلاعاتی در سازمان‌ها منجر شده است تا سیستم‌های مدرن با کاربردهای نرم‌افزاری و سخت‌افزاری بالاتر، جایگزین سیستم‌های اطلاعاتی سنتی شوند. فن‌آوری‌های

عوامل اثربخشی سیستم‌های اطلاعاتی

مطالعه‌های متعددی برای بررسی عوامل اثرگذار بر موفقیت سیستم‌های اطلاعاتی انجام شده است که یکی از مهم‌ترین آن‌ها مطالعه دلون و مک لین^{۱۱} (۱۹۹۲) است. این دو نویسنده اذعان می‌دارند، مطالعه‌های زیادی در طول دهه گذشته درباره عوامل اثرگذار بر موفقیت سیستم‌های اطلاعاتی انجام شده است؛ بدین ترتیب که پژوهشگران گوناگون جنبه‌های متفاوتی از موفقیت را در نظر گرفته‌اند که این امر به نوبه خود مقایسه را دشوار ساخته است. این دو پژوهشگر برای سازماندهی پژوهش‌های متعدد و ارائه دیدگاهی جامع‌تر از مفهومی موفقیت سیستم‌های اطلاعاتی، طبقه‌بندی جامعی را ارائه داده‌اند. این طبقه‌بندی، شش بعد را در موفقیت سیستم‌های اطلاعاتی دخیل می‌داند که عبارتند از: کیفیت سیستم، کیفیت اطلاعات، استفاده، رضایت استفاده‌کننده، اثر فردی و اثر سازمانی.

امنیت اطلاعات

همان‌گونه که گفته شد، یکی از مسائل کلیدی سیستم‌های اطلاعاتی و به طور کلی یکی از مسائل مهم هر سازمانی، امنیت اطلاعات است. هر سازمان برای ادامه حیات و بقای خود نیازمند کسب اطلاعات گوناگون و حفاظت از اطلاعات و اسرار خود می‌باشد و بعضاً دستیابی یا نشر اطلاعات سیستم باعث نابودی آن سیستم می‌گردد. امنیت اطلاعات و سیستم‌های اطلاعاتی یک مسأله حیاتی است که امروزه سازمان‌ها در سراسر دنیا با آن رو به رو هستند. معمولاً در تعاریف امنیت سیستم‌های اطلاعات، سه مؤلفه به عنوان مبانی اصلی اثربخش در امنیت اطلاعات معرفی می‌شوند:

- قابلیت اعتماد: اطمینان یافتن از اینکه اطلاعات تنها برای آن‌هایی که مجاز به دستیابی هستند، در دسترس است.
 - تمامیت (انسجام): محافظت کردن از درستی و کامل بودن اطلاعات و روش‌های پردازش.
 - در دسترس بودن: اطمینان یافتن از اینکه کاربران مجاز، به هنگام نیاز، به اطلاعات و دارایی‌ها دست می‌یابند. دستیابی به این فاکتورها را اثربخشی امنیت سیستم‌های اطلاعاتی می‌نامند.
- امنیت اطلاعات ترکیبی از سیستم‌ها و روش‌های کنترل داخلی است که باعث می‌شود محرمانگی اطلاعات و یکپارچگی و در دسترس پذیری آن حفظ شود و در ضمن راحتی کار، از اطلاعات در برابر خطرات و آسیب‌پذیری‌های موجود حفاظت می‌کند.

حسابرسی داخلی

حسابرسی داخلی یک حرفه تخصصی است که در پاسخ به رشد، توسعه و پیچیدگی سازمان‌ها تکوین و تکامل یافته است و با خدمات اطمینان بخشی و مشاوره در حوزه‌های ریسک، کنترل و راهبری، ارزش آفرینی می‌کند. اعتبار و شهرت پایدار این حرفه ایجاب می‌کند که چارچوب مشخصی برای فعالیت‌های حرفه‌ای تدوین شود.

در بیشتر سازمان‌ها هر دو بخش حسابرسی داخلی و سیستم اطلاعاتی یا ایمنی اطلاعات در تعامل هستند. بخش ایمنی اطلاعات، مسئولیت طراحی، استقرار و حفظ برنامه ایمنی اثربخش و مقرون به صرفه اطلاعات را برعهده دارد. حسابرسی داخلی یک بررسی و تحلیل مستقل از کارهای ایمنی اطلاعات سازمان ارائه می‌کند. در حالت ایده‌آل بازخورد ارائه شده توسط حسابرسی داخلی می‌تواند برای ارتقاء اثربخشی کلی ایمنی اطلاعات سازمان کاربرد داشته باشد. این دو بخش می‌بایست به صورت هم‌افزا با یکدیگر کار کنند تا اثربخشی کلی ایمنی اطلاعات سازمان را به حد عالی برسانند.

ارتباط ضعیف، نادرست یا ناکافی بین حسابرسی داخلی و ایمنی اطلاعات می‌تواند یک اثر منفی روی فعالیت این واحدها داشته باشد. در واقع شواهد قابل ملاحظه‌ای وجود دارد که مشکلات ارتباطی بیشتر مربوط به تفاوت‌های بین سابقه و دانش است که زیربنای بیشتر عدم توافق‌هاست و اغلب بین مدیر مالی و مدیر فناوری اطلاعات رخ می‌دهد.

تحقیقات نشان داده‌اند که مدیران ارشد، به عنوان یکی از اعضای تصمیم‌گیرنده در درون سازمان، بر رفتار حرفه‌ای کارکنان تاثیر می‌گذارد و موجب می‌شود تا ارزش‌های شخصی به ارزش‌های سازمانی تبدیل شود (حقیقی نسب و همکاران، ۱۳۹۵).

پژوهش داخلی

راشدی اصل و خاتم زاده (۱۳۹۶) تحقیقی با عنوان بررسی رابطه بین حسابرسی داخلی و امنیت اطلاعات در شرکت‌های صنعتی را انجام داده‌اند. جامعه آماری این تحقیق حساب‌رسان داخلی در شرکت‌های صنعتی پذیرفته شده در بورس اوراق بهادار تهران در سال ۱۳۹۶-۱۳۹۵ می‌باشد که تعداد آن‌ها ۱۲۰ نفر می‌باشد. حجم نمونه از جدول مورگان ۹۲ نفر انتخاب شد. در این تحقیق از روش نمونه‌گیری غیر تصادفی (در دسترس) استفاده شد. ابزار مورد استفاده در این پژوهش، پرسشنامه بود. به منظور تجزیه و تحلیل داده‌های پژوهش، روش‌های آماری توصیفی نظیر میانگین، انحراف معیار، میانه، مد و روش‌های استنباطی آزمون ضریب همبستگی پیرسون و رگرسیون چندگانه استفاده شده است. داده‌پردازی نیز با استفاده از نرم‌افزار SPSS انجام شد. پژوهش حاضر نشان داد که بین حسابرسی داخلی و امنیت اطلاعات در شرکت‌های صنعتی پذیرفته شده در بورس اوراق بهادار تهران رابطه مثبت و قوی معناداری وجود دارد. نتایج کلی رگرسیون نشان داد با توجه به اینکه سطح معنی‌داری، پایین‌تر از ۰,۰۱ می‌باشد خطی بودن رابطه بین متغیرها در رگرسیون معنادار می‌باشد. با توجه به مقادیر به دست آمده میزان تاثیر متغیر سطح دانش فناوری اطلاعات بر امنیت اطلاعات از پنج متغیر دیگر بیشتر می‌باشد و متغیر ویژگی‌های سازمانی دارای کمترین میزان اهمیت می‌باشد.

سعیدی (۱۳۹۵) تحقیقی با عنوان بررسی رابطه بین حسابرسی داخلی و امنیت اطلاعات در سطح دانشگاه‌های شهرستان سمنان را انجام داده است. جامعه آماری این تحقیق کارکنان بخش مالی و بخش IT دانشگاه بودند که تعداد آن برابر ۱۲۸

نفر بوده و تعداد ۹۶ نفر به عنوان نمونه آماری با استفاده از فرمول کوکران انتخاب گردیدند. از پرسشنامه جهت جمع‌آوری داده‌ها استفاده گردیده است. پایایی پرسشنامه با استفاده از ضریب آلفای کرونباخ محاسبه شده و مقدار آن برای هر یک از ابعاد بالاتر از ۰.۷۰٪ شد. برای تجزیه و تحلیل داده‌ها در ابتدا با استفاده از آزمون کولموگروف-اسمیرنوف نرمال بودن متغیرهای تحقیق مورد بررسی قرار گرفته است که با توجه به نرمال بودن داده‌ها با استفاده از آزمون تی تک عاملی و آزمون فریدمن به آزمون فرضیه‌های تحقیق پرداخته شده است. نتایج حاصل از تحقیق نشان می‌دهد دانش IT حسابرس داخلی بیشترین تاثیر را بر رابطه بین دواير حسابرسی داخلی و امنیت اطلاعات داشته است. بعد از آن حمایت مدیران ارشد، سپس ویژگی‌های سازمانی و بعد از آن مهارت‌های ارتباطی حسابرسان و در آخر نیز نگرش حسابرسان داخلی کمترین تاثیر را بر رابطه بین دواير حسابرسی داخلی و امنیت اطلاعات داشته است. تمامی فرضیات در سطح ۰.۹۵٪ اطمینان تایید گردید. بنابراین بین حسابرسی داخلی و امنیت اطلاعات رابطه معناداری وجود دارد.

نظامی (۱۳۹۵) تحقیقی با عنوان بررسی تاثیر حمایت مدیران ارشد در تمایل به استفاده از سیستم‌های اطلاعات بیمارستانی توسط پرستاران (ورد مطالعه: مرکز آموزشی پژوهشی درمانی آیت الله طالقانی مشهد) را انجام داده است. این پژوهش با هدف شناسایی تاثیر حمایت مدیران ارشد در تمایل به استفاده سیستم‌های اطلاعات بیمارستانی در میان پرستاران مرکز آموزشی پژوهشی درمانی آیت الله طالقانی مشهد انجام گرفته است. ماهیت این پژوهش پیمایشی بوده و جامعه آماری آن را، پرستاران مرکز آموزشی پژوهشی درمانی آیت الله طالقانی تشکیل داده که بر این اساس ۱۰۵ پرسشنامه توزیع و سپس جمع‌آوری شد. در این مطالعه جهت بررسی فرضیه‌های تحقیق، از مدل‌یابی معادلات ساختاری استفاده شده است. در این راستا نرم‌افزارهای SPSS18 و AMOS مورد استفاده قرار گرفت. نتایج حاصل از این تحقیق بیانگر آن است که حمایت مدیران ارشد با نقش واسطه گر برداشت ذهنی از سهولت استفاده و برداشت ذهنی از مفید بودن در پذیرش سیستم اطلاعات بیمارستان تاثیر مثبت دارند.

پژوهش خارجی

اشتاینبارت و همکاران (۲۰۱۸) تحقیقی با عنوان بررسی یک رابطه خوب بین حسابرسی داخلی و امنیت اطلاعات بر نتایج امنیت اطلاعات را انجام داده‌اند. این تحقیق با استفاده از یک مجموعه داده منحصر به فرد، به بررسی تاثیر کیفیت رابطه بین کمیته حسابرسی داخلی و کمیته امنیت اطلاعات بر تلاش برای حفاظت امنیت اطلاعات و نتایج آن می‌پردازد. نتایج به دست آمده از تجزیه و تحلیل داده‌ها نشان داد که کیفیت این رابطه تاثیر مثبتی بر تعداد ضعف‌های گزارش شده کنترل داخلی و حوادث عدم رعایت و همچنین تعداد حادثه امنیتی کشف شده که قبل و بعد از آن به سازمان آسیب رسانده است، دارد. علاوه بر این، نتایج نشان داد که سطح بالاتری از حمایت مدیریت ارشد برای امنیت اطلاعات و داشتن مأمور امنیت اطلاعات اصلی (CISO) مستقل از کمیته فناوری اطلاعات، تاثیر مثبتی بر کیفیت ارتباط بین حسابرسی داخلی و عملکرد امنیتی اطلاعات دارد.

باوئر و استپ^{۱۲} (۲۰۱۶) تحقیقی با عنوان بررسی وجود یک تیم تخصصی بین حسابرسان و متخصصان فناوری اطلاعات و تاثیرات آن در فرآیند و نتایج حسابرسی را انجام داده‌اند. هدف از این تحقیق بررسی این موضوع است که روابط بین حسابرسان داخلی و متخصصان فناوری اطلاعات چه اهمیتی برای حسابرسی و گزارشگری مالی دارد. جامعه آماری این تحقیق حسابرسان داخلی و مشاوران امنیت اطلاعات ۴ سازمان بزرگ می‌باشد و داده‌ها با استفاده از مصاحبه تخصصی با این افراد گردآوری شده است. نتایج تحلیل این داده‌ها نشان می‌دهد که کیفیت ارتباط بین این دو گروه به ارتباط، اعتماد و احترام متقابل درک شده بین این دو گروه بستگی دارد. زیرا حسابرسان ادعا می‌کنند که دیدگاه یک تیم جامع و تخصصی شامل حسابرسان و متخصصان فناوری اطلاعات است ولی متخصصان فناوری اطلاعات معتقدند که حسابرسان فقط در مواقع ضروری و شرایط بد و ویژه به آن‌ها به عنوان یک تیم همراه نگاه می‌کنند. بنابراین روابط درک شده خوب و بد، ویژگی‌های متفاوتی دارد. روابط بد، متخصصان فناوری اطلاعات را کمتر درگیر اصلاح فرآیند حسابرسی در شرایط غیرمنتظره، می‌کند. به طور کلی یافته‌های این تحقیق

نشان می‌دهد که کمیته حسابرسی با کیفیت رابطه بد، ریسک یکپارچگی ضعیف، آزمون‌های ناکافی و عدم اعتماد به کمیته امنیت اطلاعات را افزایش می‌دهد و در نتیجه کیفیت گزارشگری مالی کمیته حسابرسی را مورد تهدید قرار می‌دهد. بالعکس با روابط خوب، حسابرسان و متخصصان فناوری اطلاعات انگیزه دارند که اغلب با یکدیگر ارتباط برقرار کنند و با هم کار کنند تا شکاف‌های دانش را کاهش دهند و حسابرسی را تقویت کنند.

اشتاینبارت و همکاران (۲۰۱۵) تحقیقی با عنوان تأثیر حسابرسی داخلی بر روی اثربخشی امنیت اطلاعات: ادراکات حسابرسان داخلی را انجام داده‌اند. این مطالعه نتایجی از ادراکات کمیته حسابرسی داخلی درباره ماهیت رابطه بین کمیته امنیت اطلاعات و کمیته حسابرسی داخلی و تأثیر آن رابطه در تلاش برای حفاظت از اطلاعات سازمان را ارائه می‌دهد. حسابرسان داخلی دریافته‌اند که افزایش تکرار بازنگری برخی از فعالیت‌های امنیتی اطلاعات، کیفیت ارتباط بین دو کمیته مذکور را بهبود می‌بخشد. کیفیت ارتباط بین کمیته حسابرسی داخلی و امنیت اطلاعات بر تعداد حوادث امنیتی یا تعداد یافته‌های کمیته حسابرسی داخلی مربوط به مسائل امنیت اطلاعات تأثیر نمی‌گذارد. علاوه بر این تعداد بازنگری امنیت اطلاعات بر تعداد یافته‌های حسابرسی مرتبط با امنیت اطلاعات تأثیر معناداری دارد اما بر تعداد حوادث امنیتی تأثیری ندارد.

هروکس و فورتینا^{۱۳} (۲۰۱۳) تحقیقی با عنوان عملکرد حسابرسی داخلی در حوزه مدیریت فناوری اطلاعات: چشم‌انداز جامع را انجام داده‌اند. این مطالعه از یک رویکرد جامع برای توصیف تأثیر IAF در مدیریت فناوری اطلاعات استفاده می‌کند و به بررسی تأثیر ویژگی‌های کمیته حسابرسی داخلی در این مشارکت می‌پردازد. نتایج نظرسنجی نشان می‌دهد که دخالت IAF در ساختار، فرایندها و قابلیت‌های ارتباطی مدیریت فناوری اطلاعات به طور کامل گسترش نیافته است. همچنین، منابع حسابرسی و تجربه حسابرسی با فناوری اطلاعات، کارکنان و آموزش فناوری اطلاعات/گواهینامه، و تعامل بین کمیته‌های حسابرسی داخلی و هیئت‌مدیره، درگیری کمیته حسابرسی داخلی در مدیریت کل فناوری اطلاعات را تحت تأثیر قرار می‌دهند. این ویژگی‌های IAF هر دو بعد از مشارکت IAF در مدیریت فناوری اطلاعات را به طور متفاوتی تحت تأثیر قرار می‌دهند. ابوموسی^{۱۴} (۲۰۱۱) تحقیقی با عنوان فناوری اطلاعات و کاربردهای آن در حسابرسی داخلی به یک بررسی تجربی بر روی شرکت‌ها و سازمان‌های عربستان سعودی پرداخت. نتایج نشان داد که لازم است حسابرسان داخلی، دانش و مهارت‌های سیستم‌های اطلاعاتی کامپیوتری خود را به منظور برنامه‌ریزی، هدایت، نظارت و بازنگری کار انجام شده، افزایش دهند. نتایج این تحقیق نشان می‌دهد که حسابرسان داخلی عمدتاً بر خطرهای کنترل‌های سنتی فناوری اطلاعات همچون امنیت داده‌ها، کاربردپذیری و توان حفاظت از داده‌ها توسط IT تأکید دارند و توجه کمتری به توسعه سیستم و فعالیت‌های کنترلی دارند. ارزیابی فناوری اطلاعات توسط حسابرسان داخلی به عواملی همچون اهداف حسابرسی، نوع صنعت، تعداد متخصصان حسابرسی کامپیوتری در پرسنل حسابرسی داخلی و وجود سیستم‌های حسابرسی کامپیوتری جدید بستگی دارد.

فرضیه‌های پژوهش

۱. ساختار گزارشگری امنیت اطلاعات بر اثربخشی امنیت اطلاعات تأثیر معناداری دارد.
۲. ساختار گزارشگری امنیت اطلاعات بر کیفیت رابطه بین واحد امنیت اطلاعات و حسابرسی داخلی تأثیر معناداری دارد.
۳. ساختار گزارشگری امنیت اطلاعات از طریق کیفیت رابطه بین واحد امنیت اطلاعات و حسابرسی داخلی بر اثربخشی امنیت اطلاعات تأثیر معناداری دارد.
۴. سطح حمایت مدیریت ارشد برای امنیت اطلاعات بر اثربخشی امنیت اطلاعات تأثیر معناداری دارد.
۵. سطح حمایت مدیریت ارشد بر کیفیت رابطه بین واحد امنیت اطلاعات و حسابرسی داخلی تأثیر معناداری دارد.
۶. سطح حمایت مدیریت ارشد از طریق کیفیت رابطه بین واحد امنیت اطلاعات و حسابرسی داخلی بر اثربخشی امنیت اطلاعات تأثیر معناداری دارد.

روش پژوهش

یکی از مهم‌ترین مراحل انجام هر تحقیق روش انجام آن است. اگر یک تحقیق دارای مبانی نظری بسیار قوی و داده‌های آن با دقت گردآوری شده باشد اما روش تحقیق مناسبی انتخاب نشود نتایج تحقیق غیر قابل اتکا خواهد بود. در واقع روش تحقیق مجموعه‌ای است از قواعد، ابزارهای معتبر نظام یافته‌ای برای بررسی واقعیت، کشف مجهولات و دستیابی به راه‌حل‌های مناسب برای حل مشکلات (خاکی، ۱۳۸۸، ۲۰۱). به‌طور کلی روش‌های تحقیق در علوم رفتاری را می‌توان با توجه به دو ملاک: الف) هدف تحقیق و ب) نحوه‌ی گردآوری داده‌ها تقسیم کرد.

تحقیقات علمی بر اساس هدف، به سه دسته تقسیم می‌شوند: بنیادی، کاربردی و تحقیق و توسعه. هدف تحقیقات کاربردی، توسعه دانش کاربردی در یک زمینه خاص است. به‌عبارت دیگر تحقیقات کاربردی به سمت کاربرد عملی دانش هدایت می‌شود. نتایج این نوع تحقیقات در تعلیم و تربیت، مثلاً در طراحی برنامه‌های درسی و کمک به اتخاذ تصمیم‌های مربوط به نظام آموزشی به‌کار می‌رود (سرمد و همکاران، ۱۳۷۶؛ ۷۹). از این رو پژوهش حاضر که به دنبال بررسی تاثیر رابطه خوب بین حسابرسی داخلی و امنیت اطلاعات بر نتایج امنیت اطلاعات می‌باشد، پژوهشی کاربردی محسوب می‌گردد.

از طرفی، تحقیقات بر اساس نحوه گردآوری داده‌ها، به پنج دسته تحقیقات (۱) اکتشافی، (۲) توصیفی، (۳) برآوردی، (۴) ارزش‌یابی، (۵) تبیینی (پرهیزگار و آقاجانی افروزی، ۱۳۹۰، ۲۹۲). تحقق توصیفی شامل مجموعه روش‌هایی است که هدف آن‌ها توصیف کردن شرایط یا پدیده‌های مورد بررسی است. تحقیق توصیفی، خود به پنج دسته پیمایشی، همبستگی، اقدام‌پژوهی، بررسی موردی و پس‌رویدادی یا علی-مقایسه‌ای تقسیم می‌شود (سرمد و همکاران، ۱۳۷۶، ۸۲).

با توجه به توضیحات فوق، تحقیق حاضر از نظر شیوه گردآوری داده‌ها، توصیفی است زیرا پژوهش‌گر متغیرها را دستکاری نکرده و صرفاً تأثیرات متغیرها بر یکدیگر را می‌سنجد. بدین منظور تاثیر ساختار گزارشگری امنیت اطلاعات و سطح حمایت مدیریت ارشد، بر اثربخشی امنیت اطلاعات، از طریق کیفیت رابطه بین واحد امنیت اطلاعات و حسابرسی داخلی را، که محیطی دست‌کاری نشده است، بررسی می‌کند. تحقیقات توصیفی، خود به چند دسته تقسیم می‌شوند. تحقیق حاضر، بر این اساس، هم از نوع پیمایشی بوده و هم از نوع همبستگی، محسوب می‌شود. با توجه به اینکه در این تحقیق از ابزاری نظیر پرسشنامه جهت جمع‌آوری داده‌ها استفاده شده است، لذا روش این تحقیق، از نوع پیمایشی می‌باشد. پیمایش، روشی در تحقیق اجتماعی است که فراتر از یک تکنیک خاص در گردآوری اطلاعات است، هر چند عمدتاً در آن پرسشنامه استفاده می‌شود، اما فنون دیگری از قبیل مصاحبه ساختمند، مشاهده، تحلیل محتوا ... هم به‌کار می‌روند (خاکی، ۱۳۷۸، ۲۱۲). روش اجرای تحقیق نیز به دلیل اینکه به بررسی رابطه علت و معلولی بین متغیرها در آن پرداخته شده است، از نوع همبستگی می‌باشد. نمودار ۳-۲ نیز، روش انجام این تحقیق را به طور خلاصه نشان داده است.

قلمرو تحقیق

قلمرو موضوعی تحقیق: حسابرسی داخلی و امنیت اطلاعات

قلمرو زمانی: زمستان ۱۳۹۷

قلمرو مکانی: بانک‌های پذیرفته شده در بورس اوراق بهادار تهران

این تحقیق با توجه به روش گردآوری داده‌ها یک تحقیق میدانی بوده است.

ابزار گردآوری داده‌ها نیز پرسشنامه بوده است. در این تحقیق از پرسشنامه استاندارد که سوالات آن از منابع معتبر انگلیسی ترجمه شده و مطابق با شرایط ایران بومی‌سازی می‌شود، استفاده شده است. روایی و پایایی پرسشنامه نیز با استفاده از ابزارهای معتبر سنجیده شده و سپس در بین نمونه آماری توزیع گردیده است.

جامعه آماری مطالعه حاضر شامل کلیه کارکنان واحدهای حسابرسی داخلی و امنیت اطلاعات سازمان‌های مرکزی بانک‌های پذیرفته شده در بورس اوراق بهادار تهران، می‌باشند. تعداد این بانک‌ها تا لحظه نگارش پایان‌نامه ۱۲ بانک است که اسامی آن‌ها به شرح زیر است:

انصار - خاورمیانه - ملت - پارسیان - پاسارگاد - پست بانک - صادرات - تجارت - کارآفرین - اقتصادنویین و سینا.
با توجه به اینکه، تعداد کارکنان در واحدهای حسابرسی داخلی و امنیت اطلاعات سازمان‌های مرکزی بانک‌های مذکور به‌طور متوسط، بین ۲۵ تا ۳۰ نفر، گزارش شده‌اند، لذا حجم کل جامعه مورد مطالعه، ۳۶۰ نفر، در نظر گرفته شده‌است. در پژوهش حاضر، از روش نمونه‌گیری غیر تصادفی در دسترس استفاده شده‌است. در این روش اعضای جامعه پژوهش بر اساس راحتی نسبی دسترسی به آن‌ها انتخاب می‌شوند، پس در این روش، پژوهشگر به آزمودنی‌هایی نیاز دارد که به سرعت در دسترس باشند و آمادگی پاسخ به پرسش‌ها را داشته باشند (میرزایی، ۱۳۸۹؛ ۱۸۰). با توجه به ماهیت جامعه آماری و دسترسی سخت به کارکنان واحدهای حسابرسی داخلی و امنیت اطلاعات به دلیل مشغله زیاد ایشان، از این روش جهت انتخاب نمونه مورد مطالعه، استفاده شده‌است.
در این پژوهش از روش کتابخانه‌ای برای استخراج مطالعات و از روش میدانی جهت جمع‌آوری داده‌های آماری از نمونه مورد مطالعه استفاده شده‌است.

از آنجایی که پژوهش حاضر از نوع توصیفی می‌باشد، همچون بسیاری از مطالعات توصیفی از منابع ثانویه برای روشن شدن مباحث نظری تحقیق و به دست آوردن اطلاعات مورد نیاز از روش جمع‌آوری کتابخانه‌ای به عنوان مفیدترین روش استفاده شده‌است

مدل و نحوه اندازه‌گیری متغیرهای پژوهش

برای تعیین حجم نمونه در تحقیقات از روش‌های مختلفی استفاده می‌شود. دو روش متداول برای این کار استفاده از فرمول شارل کوکران و جدول مورگان است. حجم نمونه تحقیق حاضر به دلیل اینکه تعداد جامعه مشخص است به کمک فرمول کوکران تعیین می‌گردد. فرمول کوکران برای زمانی که حجم جامعه مشخص است به صورت زیر می‌باشد.

$$n = \frac{Nz^2 p(1-p)}{N(d)^2 + z^2 p(1-p)} \quad \text{کوکران (میرزایی، ۱۳۸۸):}$$

بنابراین حجم نمونه مورد نیاز پژوهش عبارت است از :

$$n = \frac{360 * 1.96^2 * 0.5(0.5)}{360 * (0.05)^2 + 1.96^2 * 0.5(0.5)} = 186$$

روایی

به طور کلی مقصود از روایی آن است که به وسیله اندازه‌گیری واقعاً بتواند خصیصه مورد نظر را اندازه‌گیری نماید نه متغیر دیگری را. اگر وسیله اندازه‌گیری از لحاظ خصیصه مورد نظر دارای روایی کافی نباشد، نتایج پژوهش بی ارزش خواهد بود. روایی محتوا ایجاد اطمینان می‌کند که همه ابعاد و مؤلفه‌هایی که می‌توانند مفهوم مدنظر ما را انعکاس دهند، در آن سنجه وجود دارد. هر چه وجود این ابعاد و مؤلفه‌ها در سنجه، جهت انعکاس مفهوم بیشتر باشد، روایی محتوا بیشتر می‌شود (پرهیزگار و آقاجانی افروزی، ۱۳۹۰؛ ۲۲۵).

در این پژوهش جهت سنجش روایی پرسشنامه از روایی محتوا استفاده شده است و برای اطمینان از روایی بالای تحقیق، پرسشنامه در اختیار اساتید (خبرگان) قرار گرفته و اعتبار آن مورد تأیید آن‌ها قرار گرفته است، همچنین با توجه به اینکه گویه‌های پرسشنامه برگرفته از مقاله بیس پژوهش است، بنابراین، پرسشنامه به صورت استاندارد می‌باشد.

پایایی

یک آزمون زمانی دارای پایایی است که نمره‌های مشاهده و نمره‌های واقعی آن دارای همبستگی بالایی باشند، به این معنی که چنانچه نمره‌های مشاهده شده و واقعی آزمودنی‌ها در آزمودنی موجود باشد مجذور همبستگی بین این نمره‌ها، ضریب پایایی آزمون نامیده می‌شود (خاکی، ۱۳۷۸). پایایی یکی از ویژگی‌های فنی ابزار اندازه‌گیری (پرسشنامه) است. مفهوم یاد شده با این امر سر و کار دارد که ابزار اندازه‌گیری در شرایط یکسان تا چه اندازه نتایج یکسان بدست می‌دهد.

روش تجزیه و تحلیل آماری

پس از آن که پاسخ‌ها از طریق پرسشنامه، مصاحبه یا مشاهده به دست آمد، داده‌ها باید تنظیم شوند، اگر سؤال‌های بی‌پاسخ وجود داشته باشد باید با روش‌های مختلف کنترل شوند، سپس داده‌ها کدگذاری، طبقه‌بندی و کلیدگذاری شوند؛ و سپس درباره نحوه تحلیل رایانه‌ای مورد نیاز، تصمیم‌گیری شود (پرهیزگار و آقاجانی افروزی، ۱۳۹۰، ۳۳۸). و مقیاس اندازه‌گیری نیز در انتخاب روش آماری مناسب تأثیر دارد.

آمار توصیفی

آمار توصیفی، به مجموعه‌ای از روش‌هایی می‌گویند که برای سازمان‌دهی خلاصه کردن، تهیه جدول، رسم نمودار، توصیف و تفسیر داده‌های جمع‌آوری شده از نمونه آماری به کار گرفته می‌شود. یک مجموعه داده آماری شامل مجموعه‌ای از مقادیر یک یا چند متغیر است. بنابراین، آمار توصیفی شامل آن بخش از آمار است که به ویژگی‌ها و آماره‌های مربوط به نمونه آماری تحقیق می‌پردازد. این آمار اغلب در قالب آماره‌های توصیفی، جداول یک بعدی، نمودارها، شاخص‌های گرایش به مرکز (مد، میانه و میانگین) و شاخص‌های گرایش به پراکندگی (دامنه تغییرات، واریانس، انحراف استاندارد، چولگی، کشیدگی) نمایش داده می‌شود. نقش آمار توصیفی در فرایند تحلیل آماری بسیار مهم است. آمار توصیفی با خلاصه کردن داده‌ها، ویژگی‌های مهم آن را نمایان می‌سازد تا ایده‌های لازم را در ذهن پژوهش‌گر برای مرحله دوم تحلیل آماری (آمار استنباطی) ایجاد کند. به منظور شناخت بهتر ماهیت جامعه‌ای که در پژوهش مورد مطالعه قرار گرفته است و آشنایی بیشتر با متغیرهای پژوهش، قبل از تجزیه و تحلیل داده‌های آماری، لازم است این داده‌ها توصیف شود. همچنین توصیف آماری داده‌ها، گامی در جهت تشخیص الگوی حاکم بر آن‌ها و پایه‌ای برای تبیین روابط بین متغیرهایی است که در پژوهش به کار می‌رود (خورشیدی و قریشی، ۱۳۸۱، ۲۵۴).

در جدول شماره ۱ به توصیف متغیرهای تحقیق پرداخته شده است. در این جدول شاخص‌های مرکزی که شامل میانگین است و شاخص‌های پراکندگی که شامل واریانس، دامنه تغییرات و انحراف استاندارد و شاخص‌های انحراف از قرینگی که شامل چولگی و کشیدگی می‌شود را دربردارد که همگی در حد مطلوب می‌باشند.

جدول ۱: توصیف متغیرهای تحقیق

متغیر	میانگین	انحراف استاندارد	چولگی	کشیدگی
ساختار گزارشگری امنیت اطلاعات	۲/۵۱۹	۰/۷۷۸	-۰/۲۵۴	۰/۴۲۸
سطح حمایت مدیریت ارشد برای امنیت اطلاعات	۲/۵۷۷	۰/۶۱۴	-۰/۱۷۷	۰/۵۸۸
کیفیت رابطه بین واحد امنیت اطلاعات و حساسی داخلی	۲/۷۱۱	۰/۶۵۰	-۰/۵۹۸	۱/۵۹۳

۰/۱۸۶	-۰/۰۴۱	۰/۶۱۰	۲/۶۴۹	اثربخشی امنیت اطلاعات
-------	--------	-------	-------	-----------------------

آمار استنباطی و آزمون فرضیه‌ها

در این پژوهش از مدل‌یابی معادلات ساختاری برای بررسی اعتبار سازه‌ها و همچنین آزمون فرضیه‌های پژوهش استفاده می‌شود. در مجموع از تحلیل عاملی تاییدی و مدل ساختاری استفاده شده است. بدین ترتیب که ابتدا تحلیل عاملی تاییدی برای پرسش‌های پرسشنامه صورت گرفت و سپس تحلیل ساختاری عامل‌ها برای آزمون درجه تاثیرگذاری متغیر مکنون مستقل بر متغیر مکنون وابسته مورد بررسی قرار گرفت.

نتایج آزمون فرضیات

جدول ۲ نشان‌دهنده نتایج مدل‌های ساختاری پژوهش برای آزمون فرضیه‌های تحقیق می‌باشد. با توجه به مقادیر ارائه شده در این جدول، زمانیکه عدد معناداری بیش از مقدار (۱/۹۶) و یا کمتر از مقدار (-۱/۹۶) حاصل شود، در این صورت فرضیه فوق تایید می‌گردد. بنابراین، طبق جدول ۲، از ۷ فرضیه، به جز فرضیه‌های دوم و سوم، سایر فرضیه‌های این تحقیق مورد تایید واقع شده‌اند.

جدول ۲ بررسی فرضیات پژوهش

فرضیه‌ها	مسیر	ضریب مسیر	آماره تی	P-Value	نتیجه فرضیه		
۱	ساختار گزارشگری	<<<<<<	اثربخشی امنیت اطلاعات	۰/۱۶۲	۲/۱۴۳	۰/۰۳۳	تایید
۲	ساختار گزارشگری	<<<<<<	کیفیت رابطه	۰/۰۰۸	۰/۱۰۷	۰/۹۱۵	عدم تایید
۳	ساختار گزارشگری	کیفیت رابطه	اثربخشی امنیت اطلاعات	۰/۰۰۸	۰/۱۰۷	۰/۹۱۵	عدم تایید
			اطلاعات	۰/۳۷۰	۵/۳۱۵	۰/۰۰۰	
۴	سطح حمایت مدیریت ارشد	<<<<<<	اثربخشی امنیت اطلاعات	۰/۵۷۶	۳/۸۱۸	۰/۰۰۰	تایید
۵	سطح حمایت مدیریت ارشد	<<<<<<	کیفیت رابطه	۰/۶۹۷	۱۱/۲۶۹	۰/۰۰۰	تایید
۶	سطح حمایت مدیریت ارشد	کیفیت رابطه	اثربخشی امنیت اطلاعات	۰/۶۹۷	۱۱/۲۶۹	۰/۰۰۰	تایید
			اطلاعات	۰/۳۷۰	۵/۳۱۵	۰/۰۰۰	
۷	کیفیت رابطه	<<<<<<	اثربخشی امنیت اطلاعات	۰/۳۷۰	۵/۳۱۵	۰/۰۰۰	تایید

خلاصه نتایج و فرضیه‌های تحقیق

هدف اصلی از مطالعه حاضر بررسی نقش میانجیگری کیفیت رابطه بین واحد امنیت اطلاعات و حساسی داخلی در زمینه تاثیر ساختار گزارشگری امنیت اطلاعات و همچنین سطح حمایت مدیریت ارشد برای امنیت اطلاعات بر اثربخشی امنیت اطلاعات، بوده است. از این‌رو در این پژوهش تأثیر ساختار گزارشگری امنیت اطلاعات و سطح حمایت مدیریت ارشد برای امنیت اطلاعات، به عنوان متغیرهای مستقل، بر اثربخشی امنیت اطلاعات به‌عنوان متغیر وابسته، سنجیده شده است. همچنین،

کیفیت رابطه بین واحد امنیت اطلاعات و حسابرسی داخلی، به عنوان متغیر میانجی، در مسیر تأثیرات مورد بررسی، مورد آزمون قرار گرفته است.

تحقیق حاضر از نوع کاربردی می باشد زیرا هدف از انجام آن توسعه دانش کاربردی در زمینه اثربخشی امنیت اطلاعات در بانکها، می باشد. همچنین درزمینهی نحوه گردآوری داده ها نیز مطالعه حاضر مطالعه ای توصیفی از نوع پیمایشی است، همچنین به دلیل اینکه به بررسی رابطه علت و معلولی بین متغیرها، پرداخته شده است، از نوع همبستگی نیز محسوب می شود. جامعه مورد بررسی در این پژوهش، کلیه کارکنان واحدهای حسابرسی داخلی و امنیت اطلاعات سازمان های مرکزی بانک های پذیرفته شده در بورس اوراق بهادار تهران بوده اند که به روش نمونه گیری در دسترس، به انتخاب حجم نمونه ای برابر با ۱۸۶ نفر جهت مطالعه، پرداخته شده است. در این مطالعه به منظور تحلیل داده ها از دو رویکرد کلی آماری آمار توصیفی و آمار استنباطی استفاده گردید. آمار توصیفی به منظور توصیف ویژگی های جمعیت شناختی جامعه آماری در کنار سنجش شاخص های پراکندگی داده ها مورد استفاده قرار گرفت. همچنین، آمار استنباطی و روش حداقل مربعات جزئی، به منظور بررسی معناداری تأثیر مفروض متغیرها بر یکدیگر مورد استفاده قرار گرفت.

منابع و مراجع

- [۱] احمدی اسلاملو؛ فروغ حیرانی، زهرا؛ و شاهمرادی، نسیم؛ (۱۳۹۵)، بررسی تاثیر ویژگی‌های حسابرسی داخلی از دیدگاه حسابرسان و متخصصین IT بر روابط بین حسابرسی داخلی و امنیت اطلاعات، چهارمین کنفرانس بین‌المللی حسابداری و مدیریت با رویکرد علوم پژوهشی نوین، تهران، شرکت ارتباط ارغوان ایرانیان.
- [۲] اسکو، وحید؛ و سلطانی، مهدی؛ (۱۳۹۱)، بررسی تاثیر حمایت مدیریت ارشد بر عملکرد سیستم‌های اطلاعاتی با استفاده از مدل‌سازی معادلات ساختاری (مورد مطالعه: شرکت‌های صنعتی استان یزد)، کنفرانس ملی حسابداری، مدیریت مالی و سرمایه‌گذاری، گرگان، دانشگاه جامع علمی کاربردی استان گلستان.
- [۳] آذر، عادل، غلامزاده، رسول، قنواتی، مهدی. (۱۳۹۱). مدل‌سازی مسیری-ساختاری در مدیریت، تهران، نگاه دانش.
- [۴] آقای، رضا؛ آقای آقای، میلاد؛ آقای، اصغر (۱۳۹۵)، شناسایی و تبیین عوامل کلیدی موثر بر حوزه سیستم‌های اطلاعاتی مدیریت، مطالعات مدیریت کسب‌وکار هوشمند، ۴(۱۵): ۱۲۵-۱۴۸.
- [۵] پاک‌مرام، عسگر؛ رستم‌نژاد، ابراهیم؛ و قهرمانی، داریوش؛ (۱۳۹۵)، ارتباط بین حسابرسی داخلی و امنیت اطلاعات؛ تحقیق اکتشافی، مطالعات اقتصاد، مدیریت مالی و حسابداری، ۲(۲/۲): ۷۹-۸۸.
- [۶] پورجعفری، پیمان. و کیاکجوری، کریم. (۱۳۹۴). نقش فرهنگ سازمانی و حمایت مدیران ارشد در شکل‌گیری رفتار به‌اشتراک‌گذاری دانش. اولین کنفرانس بین‌المللی حسابداری، مدیریت و نوآوری در کسب‌وکار، گیلان - موسسه پویندگان اندیشه‌های نو و شهرداری صومعه‌سرا، مجتمع فرهنگی و هنری فارابی اداره فرهنگ و ارشاد.
- [۷] حسینی، سید یعقوب، یداللهی، شهربانو (۱۳۹۲). آمار پارامتریک و روش پژوهش، انتشارات صفار، چاپ اول.
- [۸] حقیقی نسب، منیژه؛ یزدانی، حمیدرضا؛ و داورپناه کیاسرایی، فاطمه؛ (۱۳۹۵)، تأثیر حمایت مدیریت ارشد از اقدامات زیست محیطی بر استراتژی بازاریابی سبز و عملکرد زیست-محیطی کسب و کارهای صنعتی در ایران، تحقیقات بازاریابی نوین، ۶(۲۰/۱): ۲۳-۳۸.
- [۹] حقیقی نسب، منیژه؛ و تقوی، سیده صفیه؛ (۱۳۹۱)، عوامل تأثیرگذار بر اشاعه کسب‌وکار الکترونیک در سازمان‌های ایرانی، مدیریت فناوری اطلاعات، ۴(۱۰): ۲۵-۴۰.
- [۱۰] خورشیدی، عباس و قریشی، حمیدرضا (۱۳۸۱)، راهنمای تدوین رساله و پایان‌نامه تحصیلی (از نظریه تا عمل)، تهران، یسطرون، ۱۳۸۱
- [۱۱] خیرگو، منصور؛ و شکوهی، جواد؛ (۱۳۹۵)، شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر اثربخشی سیستم‌های اطلاعاتی در سازمان‌های دولتی، پردازش و مدیریت اطلاعات، ۳۲(۳): ۶۹۵-۷۱۲.
- [۱۲] داوری، علی، رضازاده، آرش، (۱۳۹۶). مدل‌سازی معادلات ساختاری با نرم افزار PLS، سازمان انتشارات جهاد دانشگاهی، چهارم
- [۱۳] دلفان حسینی، شیوا؛ (۱۳۹۰)، ارتباطات سازمانی، تهران، انتشارات پردوش، چاپ اول.
- [۱۴] راشدی اصل، علی؛ و خاتم‌زاده، سیدعلی؛ (۱۳۹۶)، بررسی رابطه بین حسابرسی داخلی و امنیت اطلاعات در شرکت‌های صنعتی، کنفرانس ملی تحقیقات علمی جهان در مدیریت، حسابداری، حقوق و علوم اجتماعی، شیراز، دانشگاه آزاد اسلامی واحد زرقان - دانشگاه علمی کاربردی شوشتر.
- [۱۵] رضایی، علی؛ مصدق، محمدجواد؛ و رضایی، مونا؛ (۱۳۹۷)، عوامل مؤثر بر اثربخشی سیستم مدیریت امنیت اطلاعات، مدیریت توسعه و تحول، ۳۳(۱): ۷۳-۸۲.

- [۱۶] سعیدی، میترا، (۱۳۹۵)، بررسی رابطه بین حسابرسی داخلی و امنیت اطلاعات در سطح دانشگاه های شهرستان سنندج، مطالعات مدیریت و حسابداری ۲(۲): ۱-۱۸.
- [۱۷] سلیمانی اصل، محبوبه؛ (۱۳۹۴)، شناسایی چالش های امنیت فناوری اطلاعات در حسابرسی دیوان محاسبات کشور، دانش حسابرسی، ۱۵(۵۹): ۱۸۹-۲۱۰.
- [۱۸] سیادت، حسین؛ (۱۳۹۴)، عوامل موثر بر اثربخشی حسابرسی داخلی در بهبود امنیت اطلاعات در بانک ملی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکز، دانشکده مدیریت و حسابداری.
- [۱۹] سیفی کار جیهونی، مهشید؛ حمیدی، ناصر؛ و حسن پور، آرش؛ (۱۳۹۲)، بررسی اثربخشی مدل امنیت سیستم های اطلاعاتی در انواع سازمان، کنفرانس بین المللی مدیریت، چالش ها و راهکارها، شیراز.
- [۲۰] عارف نژاد، محسن؛ امیرخانی، طیبه؛ و سبجانی، محمد؛ (۱۳۹۱)، تبیین عوامل موثر بر موفقیت سیستم های اطلاعاتی: با تاکید بر نقش عوامل سازمانی و یادگیری سازمانی (مطالعه موردی سازمان صنایع و معادن استان اصفهان)، مدیریت فناوری اطلاعات، ۴(۱۳): ۸۹-۱۱۴.
- [۲۱] عباس پور، عباس؛ و باروتیان، هدی؛ (۱۳۸۹)، بررسی رابطه ارتباطات اثربخش و عملکرد سازمانی (بر اساس مدل اچیو) در واحدهای ستادی شرکت ملی گاز ایران در سال ۱۳۸۸، مدیریت و منابع انسانی در صنعت نفت، ۴(۱۰): ۷-۳۸.
- [۲۲] فاطمی نسب، عزت اله؛ و محمودزاده، ابرهیم؛ (۱۳۹۶)، بررسی تاثیر ارتباطات سازمانی بر تسهیم دانش در شرکت راه آهن جمهوری اسلامی ایران، مطالعات مدیریت راهبردی دفاع ملی، ۱(۱): ۷۹-۱۰۲.
- [۲۳] فرهنگی، علی اکبر؛ صفرزاده، حسین؛ (۱۳۸۴)، طراحی و تبیین الگوی ارتباطات سازمانی در فرایند کارفرینی سازمانی (با تاکید بر شرکت های پخش سراسری ایران)، دانشور.
- [۲۴] فرهنگی، علی اکبر؛ صفرزاده، حسین؛ (۱۳۸۶)، نظریه های ارتباط سازمانی، تهران، انتشارات رسا، چاپ دوم.
- [۲۵] کربلایی سلمانپور ممقانی، لید، شهم، گلسا. و درگاهی، حسین. (۱۳۹۴). بررسی سازگاری ویژگی های شخصیتی مدیران ارشد با شغل مدیریت در دانشکده های دانشگاه علوم پزشکی تهران. مجله دانشکده پیراپزشکی دانشگاه علوم پزشکی تهران (پیاورد سلامت)، ۱۹(۱): ۹۶-۸۱.
- [۲۶] لگزیان، محمد؛ ناظمی، شمس الدین؛ و دادمند، فاطمه؛ (۱۳۹۱)، ارزیابی موفقیت سیستم اطلاعاتی مالی دانشگاه فردوسی مشهد با به کارگیری مدل تعدیل شده دلون و مک لین، پردازش و مدیریت اطلاعات، ۲۷(۳): ۵۷۷-۵۹۶.
- [۲۷] ملکی رنجبر، فاطمه؛ (۱۳۸۴)، بررسی ارتباطات اثربخش درون سازمانی بر عملکرد کارکنان شرکت آب و فاضلاب همدان، پایان نامه کارشناسی ارشد، دانشکده امور اداری و مدیریت.
- [۲۸] میرکمالی، محمد؛ (۱۳۸۶)، رفتار و روابط در سازمان و مدیریت، یسطرون، تهران.
- [۲۹] نصرافهانی، غلامرضا (۱۳۹۰)، بررسی رابطه بین ارتباطات اثربخش مدیران و نمره ارزشیابی عملکرد کارکنان سازمان امور اقتصادی و دارایی استان اصفهان، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی نجف آباد.
- [۳۰] نظامی، ستاره؛ (۱۳۹۵)، بررسی تأثیر حمایت مدیران ارشد در تمایل به استفاده از سیستم های اطلاعات بیمارستانی توسط پرستاران مورد مطالعه: مرکز آموزشی پژوهشی درمانی آیت الله طالقانی مشهد، اولین همایش بین المللی انسجام مدیریت و اقتصاد در توسعه شهری، تبریز، دانشگاه اسوه، دانشگاه آتاترک ترکیه.
- [۳۱] الهی، شعبان؛ طاهری، مهدی؛ حسن زاده خوش طینت، علیرضا؛ (۱۳۸۸)، ارائه چارچوبی برای عوامل انسانی مرتبط در امنیت سیستم های اطلاعاتی، مدیریت در ایران، ۱۳(۶۱/۲): ۱-۲۲.

- [33] Abu-Musa, Ahmad A. (2011), "Information Technology and Its Implications for Internal Auditing: An Empirical Study of Saudi Organizations", *Managerial Auditing Journal*. Vol.23 No5, pp.438-466.
- [34] Al-adaileh, R.(2009), . An Evaluation of Information Systems Success: A User Perspective - the Case of Jordan Telecom Group. *European Journal of Scientific Research* 37(2): 226-239.
- [35] Alaedini, M., Salekfard, S., (2014), Investigating the role of an enterprise architecture project in the business-IT alignment, *Information systems frontiers*, 15(1), 67-88.
- [36] Alfawaz, S., (2011), Information security management: a case study of an information security culture, Phd thesis, Queensland University of technology, faculty of science and technology.
- [37] Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.
- [38] Ang C.L., Davies M.A., Finlay P.N. (2001), An empirical model of IT usage in the Malaysian public sector. *Journal of Strategic Information Systems*, 10(2); 159-174.
- [39] Atif, A., (2015), A case analysis of information systems and security incident responses, *International Journal of Information Management*, 35, 717-723.
- [40] Atkins, B., (2014), Board focus on cyber security, *corporate government*, 43(3), 308-321.
- [41] Bagchi, K. and G. Udo, (2003), An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the AIS*, 12(46): p. 684-700.
- [42] Bandura, A. (1997), Self-Efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, 84, 191-215.
- [43] Bauer, T., & Estep, C. (2016). One team or two teams? exploring relationship quality between auditors and it specialists and its implications for a collective audit team identity and the audit process. Working Paper. Available at: <http://papers.ssrn.com/sol3/papers>.
- [44] Bellone, J., (2008), A practiced approach to information security management system implementation, *Information Management & Computer Security*, 16 (1): 49-57.
- [45] Bloisi, w., cook, c. w.; hunsaker, p. L. (2003). *management and organizational behavior*. new york : McGraw Hill , european edition.
- [46] Chen, J.-c., Silverthorne, C., & Hung, J.-Y. (2006). Organizational communication, job stress, organizational commitment, and job performance of accounting professionals in Taiwan and America. *Leadership & organization Development journal* , 27, 242_249.
- [47] Chen, Jiun-Shiu., Lovvorn, Al S. (2011). The speed of knowledge transfer within multinational enterprises: the role of social capital. *International Journal of Commerce and Management*, 21(1), 46-62.
- [48] Chou, H.W., Joe, SH. B. (1999). IS key issues in Taiwan's enterprises. *International Journal of Information Management*, Vol.19, pp: 369-387.
- [49] Clopton, Aaron W. (2011). *Social capital and team performance*. *Team Performance Management*, 17(7/8), 369-381.
- [50] Crawford, C. B & Sue Strohkirch, C. (2006) "The Critical Role Of Communication In Knowledge Organizations: Communication Apprehension As A Predictor Of Knowledge Management Functions" , *Journal of Knowledge Management Practice*, Vol. 7, No. 4. <http://www.tlainc.com/articl122.htm>.
- [51] Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297-334.

- [52] Cuel, R., & Ferrario, R. (2006). The impact of technology in organizational communication processes: toward constructivism.
- [53] D'Arcy J, Hovav A, Galletta D. (2009), User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf Syst Res*;20:79–98.
- [54] Delone W.H., McLean E.R.(1992). Information systems success: The Quest for the Dependent Variable. *Information System Research*; 3(1): 90-60.
- [55] Dhillon G, Tejay G, Hong W.(2007), Identifying governance dimensions to evaluate information systems security in organizations. *Proceedings of the 40th Hawaii International Conference on Systems Sciences*.
- [56] Dittenhofer, M. A., Ramamoorti, S., Ziegenfuss, D. E., & Evans, R. L. (2010). Behavioral dimensions of internal auditing: A practical guide to professional relationships in internal auditing. Altamonte Springs, IL: The Institute of Internal Auditors Research Foundation. concerning information security. *MIS Quarterly*, 34(3), 567e594.
- [57] Erick, A., (2015), Major accident prevention and management of information systems security in technology-based work processes, *Journal of Loss Prevention in the Process Industries*, 36, 84-91.
- [58] Ernst, & Young. (2015). How boards can help crack the cybereconomics equation. *Board Matters Quarterly*, September, 14e15.
- [59] Flora, P. E., & Raj, S. (2015). Navigating Technology's top 10 Risks: Internal Audit's role. concerning information security. *MIS Quarterly*, 34(3), 567e594.
- [60] Fornell, C., & Larker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.
- [61] Forster, N. (2005). Maximum performance.
- [62] Gonzalez, Jose J Agata Sawicka, (2002), A Framework for Human Factors in Information Security, Dept. of Information and Communication Technology, Agder University College, Presented at the 2002 WSEAS Int. Conf. on Information Security, Rio de Janeiro.
- [63] Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures
- [64] Gottschalk, P., (2000). Studies of key issues in IS management around the world. *International Journal of Information Management*, Vol.20, pp: 169-180.
- [65] Gritzalis D. A (1997), baseline security policy for distributed healthcare information systems. *Computers and Security*; 16(8): 709-19.
- [66] Havelka, D., & Merhout, J. W. (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems*, 14(3), 165e192.
- [67] Henderson JC, Venkatraman N. (1999), Strategic alignment: leveraging information technology for transforming organizations. *IBM Systems Journal*; 38(2,3):472–485.
- [68] Henseler, J., Ringle, C.M., & Sinkovics, R.R., (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing* 20, 277-320.
- [69] Heroux, S., & Fortin, A. (2013). The internal audit function in information technology governance: A holistic perspective. *Journal of Information Systems*, 27(1), 189e217.
- [70] Higgs, J. L., Pinsker, R., Smith, T., & Young, G. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, 30(3), 79e98.

- [71] Hill, J. (2015). Cyberwarriors with Calculators: The role of accounting and finance professionals in a Company's cybersecurity. Available at: <http://www.accaglobal.com/gb/en/technical-activities/technical-resources/search/2015/september/cyber-threat.html>.
- [72] Hinnawi, R. S. (2011). The impact of relationship marketing underpinnings on customer's loyalty Case study - Bank of Palestine. Master's Dissertation in business administration, Faculty of commerce, The Islamic University-Gaza.
- [73] Hinson, Gary, (2003). IsecT Ltd, Human factors in information security, Innovative information security awareness programs, NoticeBored.
- [74] Hong, N. (2016). For consumers, injury is hard to prove in data-breach cases. April 26. Wall Street Journal (Online). Available at: <https://www.wsj.com/articles/forconsumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988>.
- [75] Hsu, S.H., chen, W. H., & Hsieh, M. J. (2006). Robustness testing of PLS, LISREL, EQS and ANN-based SEM for measuring customer satisfaction. Total quality management & business excellence, 17(3), 355-372.
- [76] Hua, g. sher, W. pheng, S.L. (2005). Factor affecting effective communication between building clinet and maintenance contractor. 240-251.
- [77] Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies. Strategic management journal, 20(2), 195-204
- [78] IIA. International Standards for the Professional Practice of Internal Auditing. Attribute Standard 1100—Independence and Objectivity; 2011.
- [79] ISACA. (2016). State of cybersecurity: Implications for 2016. Available at: https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf.
- [80] Ito K, Kagaya T, Kim H. (2010), Information security governance to enhance corporate value. NRI Secure Technologies.
- [81] Jacobs, G. (2006). communication for commitment in remote technical workfoces. journal of communication management , 10, 353-370.
- [82] Kakkar, A., Punhani, R., Madan, S., (2012), Implementation of ISMS and its Practical Shortcomings, International Refereed Research Journal ISSN 1839-6518, Vol. 02, No. 01, www.irj.iars.info.
- [83] Kazemi, M., Khajouei, H., Nasrabadi, H., (2012), Evaluation of information security management system success factors: Case study of Municipal organization, African Journal of Business Management, 6(14): 4982-4989.
- [84] Knapp, K. J., Marshall, T. E., Rainer, R. K., Morrow, D. W., (2005), Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC) Survey Results, Auburn University, Auburn, AL.
- [85] Kotulic, A.G. and J.G. Clark, (2004), Why There Aren't More Information Security Research Studies. Information & Management, 41(5): p. 597-607.
- [86] Kumar RL, Park S, Subramaniam C. (2008), Understanding the value of countermeasure portfolios in information security. J Manag Inf Syst;25:241-79.
- [87] Kwok, L., Longley, D., (1999), Information security management and modeling, Information Management & Computer Security, 7 (1): 30-40.
- [88] Kwon, J., Ulmer, J., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. Journal of Information Systems, 27(1), 219e236.
- [89] Li, D., Hung, W., SHA, W., (2009). Key issues in information systems management: a china's perspective. From <http://www.pacisnet.org/file/2005/332.pdf>.

- [90] Li, S. H., Yen, D. C., Chen, S. C., Chen, P. S., Lu, W. H., Cho, C.C., (2015), Effects of virtualization on information security, *Computer Standards & Interfaces*, 42; 1-8.
- [91] Lu H.P., Wang J.Y. (1997), The relationship between management styles, user participation, and system success over MIS growth stages. *Information & Management*; 32(3):203-213.
- [92] Martinez, Ricardo., Jand, Francisco., Ruiz-Palomino, Pablo. (2012). Knowledge acquisition's ediation of social capital-firm innovation. *Journal of Knowledge Management*, 16(1), 61-76.
- [93] Mathisen, J. (2004), *Measuring Information Security Awareness*. Høgskolen i Gjøvik.
- [94] Mohseni, M., (2013), Has your organization compliance with ISMS? A case study in an Iranian Bank, ArXiv preprint arXiv: 1303.0468. <ftp://arxiv.org/papers/1303/1303.0468.pdf>.
- [95] Morales, G. M.-A. (2011). Partial least squares (PLS) method: Origins, evolution and application to social science. *Communications in statistics – Theory and Methods*, 40(13), 2305-2317.
- [96] Mukherjee, B & Bhatia, A & Mukherjee, A (2012) "The Role of Business Communication in Knowledge Management Organization", Ninth AIMS International Conference on Management, January 1-4.
- [97] Nunnally, J. (1978). *Psychometric theory*, 2nd Edn. New York: McGraw-Hill.
- [98] Palvia, P.C., Palvia, S., (1992). MIS issues in India and a comparison with the United States. *International Information Systems*, pp: 101-110.
- [99] Petter S., Delone W., Mclean E. (2008), Measuring information systems success: models, dimensions, measures, and interrelationships. *European Journal of Information Systems*; 17:236–263.
- [100] Phelps D, Milne K.(2008) Leveraging IT controls to improve IT operating performance. The Institute of Internal Auditors Research Foundation.
- [101] Phelps, Danielc, (2005), information system security: self-efficacy and security effectiveness in Florida Libraries, A Dissertation submitted to the College of Information in partial fulfillment of the requirements for the degree of Doctor of Philosophy, Spring Semester.
- [102] Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, 20(1), 121e139.
- [103] Ring, T., (2013), A breach too far? *Computer Fraud & Security*, 6:5-9.
- [104] Ross, S. J. (2015). Information security matters: Stanley Baldwin's bomber. *ISACA Journal*, 5, 4e6.
- [105] Salanova, M., Grau, R. M., Cifre, E., & Llorens, S. (2000), Computer training, frequency of usage and burnout: the moderating role of computer self-efficacy. *Computers in Human Behavior*, 16, 575-590.
- [106] Saunders C.S., Jones J.W. (1992), Measuring performance of the information systems function. *Journal of Management Information Systems*; 8(4): 63-73.
- [107] Siponen, M., Willison, R., (2009), Information security management standards: Problems and solutions, *Information & Management*, 46 (5): 267-270.
- [108] Soomro, Z., Shah, M., Ahmed, J., (2016), Information security management needs more holistic approach: A literature review, *International journal of management*, 36: 215-225.
- [109] Spears JL, Barki H. (2010), User participation in information systems security risk management. *MIS Q*;34:503–22.

- [110] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems*, 27(2), 65e86.
- [111] Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, 13(3), 228e243.
- [112] Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. (2015). The influence of internal audit on information security Effectiveness: Perceptions of internal auditors. <http://papers.ssrn.com/sol3/papers>.
- [113] Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. (2018), The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*.
- [114] Tabachnick, B.G., & Fidell, L.S. (2007). *Using multivariate statistics*. Boston: Person Education.
- [115] Tallon P.P., Kraemer K.L., Gurbaxani V. (2000), Executives' perceptions of the business value of information technology: A process-oriented approach. *Journal of Management Information Systems*; 16(4): 145-173.
- [116] ThreatTrack. (2016). Security analysts say defending against advanced malware still a major struggle. Available at: <http://www.threattracksecurity.com/resources/white-papers/security-analysts-say-defending-against-advanced-malwarestill-a-major-struggle.aspx>.
- [117] Tokdemir, G. (2009). *An Assessment Model for WEB-BASED Information System Effectiveness*. A Thesis Submitted To The Graduate School Of Informatics Of The Middleeast Technical University, In Partial Fulfillment Of The Requirements For The Degree Of Doctor Of Philosophy.
- [118] Vermeulen, C., Von Solms, R., (2002), The information security management toolbox taking the pain out of security management, *Information management & computer security*, 10 (3): 119-125.
- [119] von Solmsa, Basie, (2005), Rossouw von Solms, From information security to business security?, *Computers & Security*, 24; 271-273.
- [120] Wallace L, Lin H, Cefaratti MA. (2011), Information security and Sarbanes–Oxley compliance: an exploratory study. *J Inf Syst*;25:185–212.
- [121] Wetzels, M., Odekerken-Schroder, G., & Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly*, 33(1), 177
- [122] Wold, H.O. (1974). Causal flows with latent variables: Partings of the ways in the light of NIPALS modeling. *European Economic Review*, 5(1), 67-86.
- [123] Wong, A. & Sohal, A. (2007). Customer-salesperson relationships: the effects of trust and commitment on relationship quality. Working paper Faculty of Business and Economics, Monash University.
- [124] Yang, Jing., Alejandro, Thomas G. Brashear., Boles, James S. (2011). The role of social capital and knowledge transfer in selling center performance. *Journal of Business & Industrial Marketing*, 26(3), 152-161.