شناسایی، تحلیل و رتبه‌بندی عوامل موثر کلیدی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان‌های حاکمیتی (مطالعه موردی: سازمان بنادر و دریانوردی)

سعید خیری[1*]

تاریخ دریافت: ۹۴/۱۰/۲۲ *نویسنده مسئول تاریخ پذیرش: ۹۴/۱۲/۱۳

چکیده

با توجه به نقش فزاینده امنیت اطلاعات در اداره هر جامعه، سازمان‌ها و نهادهای دولتی و خصوصی ناگزیر به تأمین زیرساخت‌های لازم برای تحقق این امر مهم می‌باشند. برای اجرای بهینه و موفق سیستم‌های مدیریت امنیت اطلاعات علاوه بر منابع مادی، تکنیک‌های مدیریتی نیز تأثیر زیادی دارند. ثبت استانداردهای مدیریتی در حوزه امنیت اطلاعات فاوا می‌تواند به صورت برنامه‌ریزی‌شده طراحی شود تا وضعیت امنیتی سازمان‌ها متناسب با نیاز آن سازمان تغییر یابد و امنیت از منظر ادامه کسب‌وکار و تا اندازه‌ای در سطوح دیگر (مدیریت بحران و جنگ نرم) تضمین شود.

علی‌رغم تحقیقات گسترده در این خصوص متأسفانه به دلایل مختلف از جمله سطوح امنیتی موضوع برای نهادهای دولتی و غیردولتی و یا رابطه مستقیم حوزه مربوطه با منافع ایشان، اطلاعات شفاف و مفیدی در خصوص نحوه پیاده‌سازی و اولویت‌بندی لازم از منظر پیاده‌سازی و استقرار یک سیستم طی سال‌های گذشته تا امروز صورت نگرفته است. لذا در این تحقیق سعی شده است ضمن حفظ اطلاعات طبقه‌بندی‌شده سازمان، اطلاعات غیرمحرمانه‌ای که می‌تواند موجب ارتقای سازمان‌های مشابه شود در اختیار دیگران قرار گیرد. این پژوهش با مطالعات کتابخانه‌ای و مرور پایان‌نامه‌های مرتبط آغاز شد و پس از کسب اطلاعات مهم و پایه در خصوص موضوع مطروحه، با خبرگان و متولیان موضوع پژوهش مصاحبه شد و مجموعه‌ای از "شاخص‌های کلیدی" به دست آمد و در گروه‌های متناسب با نام "عوامل موثر کلیدی در پیاده‌سازی سیستم مدیریت امنیت" دسته‌بندی گردید و توسط ابزار پرسشنامه مورد تحلیل و ارزیابی قرار گرفت. تعداد ۱۲۶ پرسشنامه در کلیه بنادر توزیع و جمع‌آوری شد و سپس آزمون‌های مورد نیاز آماری بر روی آنها انجام گرفت. نتایج به‌دست آمده انجام سازمان مرکزی را متقاعد نمود تا نسبت به برگزاری دوره‌های آموزشی مرتبط و بازآموزی موضوع سیستم امنیت اطلاعات و برنامه‌ریزی و تخصیص رسانه و نرم‌افزار اقدام نماید.

واژه‌های کلیدی: سیستم مدیریت امنیت اطلاعات، مدیریت ریسک، امنیت اطلاعات، آسیب پذیری، میزان شدن آسیب‌پذیری.

۱. کارشناس ارشد مدیریت فناوری اطلاعات Saeedkheiri@pmo.ir

۱- مقدمه

با توجه به نقش اطلاعات به عنوان کالایی استراتژیک و با ارزش در تجارت و امنیت، امروزه لزوم حفاظت از آن ضروری به نظر می‌رسد. برای دستیابی به این هدف هر سازمان بسته به سطح اطلاعات (از نظر ارزش اقتصادی و رقابتی) نیازمند طراحی سیستم مدیریت امنیت اطلاعات مخصوص به‌خود می‌باشد تا از این طریق بتواند از سرمایه‌های اطلاعاتی خود حفاظت نماید. با توجه به اینکه امروزه داده‌ها در قالب‌های الکترونیکی و رویه‌های غیرمشهود و خودکار جریان دارند (J. Laudon, K.C. Laudo , J.P. Laudan, 2006) توجه روزافزون به مباحث مدیریت امنیت اطلاعات از طریق بر قراری قوانین و ضوابط ملی/ منطقه‌ای و همچنین توجه به راهبردهای جدید به منظور پاسخگویی به انتظارات و الزامات طرف‌های ذینفع نسبت به اطمینان از امنیت و ایمنی شبکه‌ها و سیستم‌های اطلاعاتی، باعث پدید آمدن استانداردهایی برای استقرار سیستم‌های مدیریت اطلاعات شده است.

بدیهی است هدف از استانداردسازی مدیریت امنیت اطلاعات و ایجاد رویکردی مشابه و حتی‌الامکان یکسان در درون سازمان‌ها جلوگیری از خلأهای امنیت اطلاعات، اتلاف منابع مالی و پیشگیری از تنش‌های ناشی از آن است. اجرای "سیستم مدیریت امنیت اطلاعات" اگرچه موجب ارتقای حفظ و به‌روزرسانی اطلاعات یک سازمان می‌شود اما پیاده‌سازی و اجرای آن همواره مشکلات خاص خود را دارد. چه‌بسا سازمان‌ها و مراکزی که در اجرای آن در کشور پیشگام بوده‌اند اما نتیجه مطلوبی به‌دست نیاورده‌اند. با وجود وضعیت نامعلوم اقتصادی و محدودیت‌های بودجه، مدیران امنیت فناوری اطلاعات بیش از گذشته نیاز دارند تا ارزش کسب و کار خود و تأثیر آن بر کاهش هزینه‌های امنیتی را به نمایش بگذارند. شناسایی و رتبه‌بندی عوامل کلیدی موثر در اجرای سیستم مدیریت امنیت اطلاعات برای سازمان‌های تخصصی و بین‌المللی بزرگی مانند "سازمان بنادر و دریانوردی" که نقش حاکمیتی سواحل و بنادر کل کشور را دارد و دارای ستاد، مراکز و بنادر متعددی در شمال و جنوب مرزهای کشور است، فوق‌العاده کاربردی می‌باشد. سازمان بنادر و دریانوردی به عنوان یک مرجع حاکمیتی بین‌المللی با مسئولیت نگهداری سواحل و بنادر و اجرای دریانوردی امن به عنوان شاه‌کلید صادرات و واردات با مخاطبان زیادی در داخل و خارج از کشور در تماس است. بنابراین حفظ و ایجاد بستر امن اطلاعاتی در کنار مجموعه عوامل محیطی دیگر مانند فاصله تا مقصد و مسیر تردد کشتی‌ها، میزان ظرفیت تخلیه و بارگیری، دپوی واردات و صادرات و غیر آن موجب ایجاد بازاری رقابتی در زمینه سرمایه‌گذاری و کسب و کار بین بنادر کشور می‌باشد.

۱-۲- اهداف

از آنجا که پیاده‌سازی و حفظ پویایی "سیستم مدیریت امنیت اطلاعات" در کلیه بنادر با توجه به هزینه و زمان امری حیاتی است، ضرورت دارد این طرح پژوهشی برای مجموعه سازمان بنادر و دریانوردی که یکی از سازمان‌های حاکمیتی کشور است انجام شود. لذا اهداف کلیدی و اساسی این پژوهش عبارتند از: (۱) شناسایی دارایی‌های امنیتی مشترک مجموعه سازمان بنادر و دریانوردی در حوزه فناوری اطلاعات، (۲) استخراج عناصر کلیدی پیاده‌سازی موفق "سیستم امنیت اطلاعات" از نگاه خبرگان موضوع در محیط سازمان بنادر و دریانوردی، (۳) تدوین یک دستورالعمل بومی در خصوص اجرا و نگهداشت "سیستم امنیت اطلاعات" و (۴) التزام و تاکید بر اهمیت اجزای موضوع در زمان بهینه با کمترین خطا.

۱-۳- تشریح سیستم مدیریت امنیت اطلاعات

الزامات و ملاحظات استاندارد ISMS[۲] به عنوان یکی از چهارچوب‌های سیستم مدیریت امنیت اطلاعات چه باهدف یک راهکار داخلی و چه باهدف اخذ گواهینامه ISO 27001 نیازمند دنبال کردن یک رویکرد ساختارمند، توجه به دامنه کسب‌وکار و داشتن درک درستی از مخاطرات امنیتی کسب‌وکار سازمان می‌باشد. استقرار ISMS یا همان مدیریت امنیت اطلاعات این فرصت را فراهم می‌آورد تا : (۱) دارایی‌های اطلاعاتی شناسایی شوند، (۲) دارایی‌های اطلاعاتی بر اساس متدولوژی های ارزش‌گذاری شوند، (۳) دارایی‌های اطلاعاتی طبقه‌بندی و برچسب‌گذاری شوند، (۴) مسئولیت دارایی‌های اطلاعاتی شفاف شود، (۵) خطرها و تهدیدها شناسایی شوند، (۶) کنترل‌های امنیتی انجام گیرد تا میزان تهدیدها و خطرها به سطح تعیین‌شده کاهش یابند، (۷) برنامه زمان‌بندی‌شده به همراه روش اجرایی برای ممیزی و بازنگری در همه موارد بالا تدوین شود، (۸) برنامه

2 - Information Security Management System

زمان‌بندی‌شده به همراه روش اجرایی برای آموزش در همه موارد بالا تدوین شود، (۹) برنامه مقابله با خطرات امنیتی تدوین و مسئولیت‌ها شفاف شود و (۱۰) سیاست‌های امنیتی، چهارچوب‌ها ، روش‌های اجرایی، راهنماها و پیشنهادات مشخص و مدون شوند.

۱-٤- بیان مسئله

مسئله ما در این تحقیق،، عدم وجود مدلی جامع در خصوص پیاده‌سازی یک سیستم مدیریتی می‌باشد. در این رابطه ابتدا تعاریفی از امنیت ، امنیت اطلاعات، تهدیدات و طریقه شناسایی آن مطالعه شد و سپس به جمع‌آوری تهدیدات حوزه‌های مختلف با دیدگاه ادامه کسب‌وکار سازمان پرداخته شد. البته در جریان مطالعه، دیدگاه‌های مدیریت بحران و پدافند غیرعامل را نیز مدنظر قرار گرفت. سپس در مورد "سیستم مدیریت امنیت اطلاعات " و راهکارهای مربوطه بحث شد، و دست‌آخر این مسئله بررسی شد که چگونه امنیت را نهادینه و کاربردی کنیم تا کسب‌وکار سازمان در ابعاد محرمانگی، یکپارچگی و دسترس‌پذیری حفظ شود و چرخه ISMS شروع و تداوم یابد. همچنین به صورت موازی مروری شد بر پیاده‌سازی سیستم‌های مشابه که هم نقش مدیریتی داشته و هم به‌عنوان یک نرم‌افزار کاربردی در حوزه فناوری اطلاعات به‌کار می‌روند. از این‌رو در تشریح مسئله، پس از توضیح مؤلفه‌های "سیستم مدیریت امنیت اطلاعات" و شناسایی شاخص‌های کلیدی، ضمن مرور تعاریف و استانداردهای موجود مرتبط، عوامل موثر (x) شناسایی شد و میزان همبستگی آنها از نظر خبرگان، کارشناسان و محیط با اجرای موفق (y) به تصویر کشیده شد. دست‌آخر، این عوامل در قالب پرسشنامه‌ای پویا در سنجش کارشناسان حوزه مدیریت امنیت اطلاعات که تجربه پیاده‌سازی را قبلاً داشته‌اند یا در جریان اجرای این سیستم بودند قرار گرفت و پس از تحلیل مطالب و رتبه‌بندی عوامل موفقیت، مدلی کاربردی جهت اجرای پویا و نمونه‌ای موفق برای مراکز حاکمیتی تهیه شد.

۱-۵- چارچوب نظری

رعایت الزامات و ملاحظات استاندارد ISMS به عنوان یکی از چهارچوب‌های سیستم مدیریت امنیت اطلاعات چه باهدف یک راهکار داخلی و چه باهدف اخذ گواهینامه ISO 27001 نیازمند دنبال کردن رویکردی ساختارمند، توجه به دامنه کسب‌وکار و داشتن درک درستی از مخاطرات امنیتی کسب‌وکار سازمان است.

۲- روش‌شناسی پژوهش

۲-۱- روش تحقیق

این تحقیق از نظر هدف کاربردی است و از نظر جمع‌آوری اطلاعات از نوع توصیفی و پیمایشی است و با توجه به اینکه این تحقیق به بررسی میزان تغییرات یک شاخص در عملکرد نتیجه (رابطه متغیرها) می‌پردازد از نوع همبستگی بوده و نوعی مطالعه موردی نیز می‌باشد. از آنجا که در این پژوهش جهت دستیابی به اهداف تحقیق و شناسایی رتبه بندر و عوامل موثر در پیاده‌سازی "سیستم مدیریت امنیت اطلاعات" است، خبرگان موضوع به صورت انتخابی تعیین شدند و داده‌های به‌دست‌آمده بدون دست‌کاری گردآوری شد، تحقیق از نوع غیر آزمایشگاهی است. همچنین از این نظر که با هدف اجرا در تمامی بنادر زیرمجموعه سازمان بنادر و دریانوردی انجام شده است، یک تحقیق کاربردی می‌باشد. برای شناسایی و رتبه‌بندی شاخص‌های کلیدی حوزه مدیریت امنیت اطلاعات با توجه به فرضیات تحقیق، ابتدا از روش کتابخانه‌ای جهت گردآوری داده‌ها استفاده شد. سپس به روش میدانی، داده‌ها کامل گردید. هدف از به‌کار گیری این روش، کشف عوامل زیربنایی بود. پرسشنامه‌ها در راستای سئوالات اصلی و فرعی طراحی شد و در نهایت به منظور ارائه مدل و دسته‌بندی متغیرها از تحلیل عامل اکتشافی و جهت آزمون فرضیه اول از روش آماری دلفی و فرضیه دوم رتبه‌بندی فریدمن و از نرم‌افزار SPSS استفاده شد.

۲-۱- ابزار و اعتبارسنجی

ابزار تحقیق در پژوهش حاضر پرسشنامه است. در این پرسشنامه سعی شده است با توجه به نظر خبرگان و متخصصان در مورد در روابط و معیارها، شاخص‌های نهایی تعیین و در بین کارشناسان متخصص مرتبط شود.

از آنجا که در پرسشنامه طراحی‌شده، سئوالات از مقیاس‌های نسبی بهره‌مند بودند، مطابق جدول (۱) مبادرت به استفاده از طیف لیکرت شد و به ترتیب برای گزینه‌های خیلی زیاد ،زیاد، متوسط، کم و خیلی کم ضرایب ۱، ۲، ۳، ۴ و ۵ در نظر گرفته شد. بدین ترتیب اطلاعات کیفی و ناپارامتریک با مقادیر کمی و عدد پی تعبیر شدند و در محاسبه‌ها ملاک عمل قرار گرفتند. از مقیاس لیکرت برای تعیین اهمیت هر عنوان از متغیرها استفاده شد. لازم

به ذکر است که در این بخش از تحقیق برای انجام تست اولیه مجموعاً تعداد ۴۴ پرسشنامه بین خبرگان و متخصصین توزیع شـد کـه ۳۱ پرسشـنامه عودت داده شد.

میزان عامل اندازه‌گیری	نظر کارشناسان و متخصصین
۵	خیلی زیاد
۴	زیاد
۳	متوسط
۲	کم
۱	خیلی کم

جدول (۱): مقیاس لیکرت پرسشنامه

بدین منظور نمونه‌های اولیه شامل نمونه‌های ۲۵ نفره و ۳۰ نفره دو بار پرسشنامه پیش‌آزمون را تکمیل کردند و سپس با استفاده از داده‌های به‌دست آمده از این پرسشنامه‌ها و به کمک نرم‌افزار آماری SPSS 21 میزان ضریب اعتماد با روش آلفای کرونباخ به شرح جدول (۲) محاسبه شد.

متغیرهای تحقیق	تعدادسئوالات	آلفای کرونباخ نمونه ۲۵ نفره	آلفای کرونباخ نمونه ۳۰ نفره
عوامل فناوری و تکنولوژی	۱۵	۰.۹۱۶	۰.۹۱۴
عوامل سازمانی یا درونی	۱۳	۰.۹۳۶	۰.۹۲۷
عوامل خارجی یا بیرونی	۵	۰.۷۷۳	۰.۷۲۰
اثربخشی و موفقیت پیاده‌سازی **ISMS**	۳	۰.۸۴۷	۰.۸۵۸
متغیر مستقل	۳۳	۰.۹۵۷	۰.۹۵۲
متغیر مستقل و وابسته	۳۶	۰.۹۶۱	۰.۹۵۸

جدول (۲): میزان آلفای کرونباخ متغیرهای تحقیق

از آنجا که مقدار به دست آمده آلفای کرونباخ برای همه متغیرهای تحقیق بالای ۰/۷ می‌باشد می‌توان گفت پرسشنامه از پایایی قابل قبولی برخوردار است.

۲-۲- سئوالات و فرضیات تحقیق

سؤالات این تحقیق را می‌توان در دو زیرگروه اصلی و فرعی به شرح زیر طبقه‌بندی نمود.

سئوال اصلی

عوامل کلیدی موثر در اجرا و پیاده‌سازی موفق سیستم مدیریت امنیت اطلاعات (ISMS) کدام‌اند؟

سئوالات فرعی

رتبه‌بندی شاخص‌های پیاده‌سازی سیستم مدیریت امنیت اطلاعات چگونه است؟

اولویت عوامل کلیدی موثر در اجرا و پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان بنادر و دریانوردی چگونه است؟

فرضیات تحقیق

برخی از فرضیات اساسی این تحقیق به شرح زیر است:

عوامل کلیدی، در پیاده‌سازی و اجرای مستمر سیستم مدیریت امنیت اطلاعات (ISMS) تأثیر می‌گذارد.

تأثیر عوامل کلیدی موفقیت در اجرا و پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) متفاوت‌اند.

۳- تجزیه و تحلیل داده‌ها

۳-۱- جایگاه چرخه مدیریتی دیمینگ در پیاده‌سازی

ایجاد امنیت یک فرایند پیچیده است. متد و مدل PDCA ساختاری است برای پیاده‌سازی سیستم ISMS. در پیاده‌سازی سیستم مذکور با پذیرش یک چرخه طرح‌ریزی (برنامه‌ریزی) مستمر که طرح را به‌روز نگه می‌دارد، می‌توان شانس خود را افزایش داد و این کار باید شامل جلسات منظم طرح‌ریزی که دربرگیرنده افراد کلیدی کسب‌وکار به منظور پیشرفت و شناسایی روش‌های بهبوددهنده طرح و عملیات است، باشد. بهبود مستمر و جستجو برای بهتر ساختن عملیات و انجام سریع‌تر و آسان‌تر و ارزان‌تر کارها، باعث تغییر و بهبود آن می‌شود. کسب‌وکارهایی که مصمم به بهبود مستمر و بازبینی طرح‌شان هستند از تجربیات گذشته برای بهبود آینده استفاده می‌کنند. تأمل در مورد رخدادهای گذشته، به مدیریت بهتر رخدادهای آینده کمک می‌کند. به این منظور می‌توان یکی از مدل‌های بهبود مستمر را که در دسترس می‌باشد به‌کار برد که معروف‌ترین آنها مدل PDCA می‌باشد .

۳-۲- شاخص‌های کلیدی موثر (CSFs) در پیاده‌سازی ISMS

شاخص‌های کلیدی موثر آن دسته از عواملی هستند که سازمان برای رقابت موفقیت‌آمیز و یا جهت مدیریت زمان و هزینه‌های خود نیازمند تمرکز و توجه به آنهاست. در مدیریت امنیت اطلاعات CSFs شرایطی است که به منظور اجرای موفق باید برآورده شوند. شناسایی شاخص‌های کلیدی منجر به اطمینان از اعمال توجه لازم به زمینه‌هایی است که موجب موفقیت می‌شوند. هدف این بخش فراهم‌سازی دانش لازم درباره شاخص موثر در پیاده‌سازی موفق سیستم مدیریت امنیت می‌باشد.

اگر مشکلات اجرای سیستم مدیریت امنیت اطلاعات در یک سازمان را تلفیقی از اجرای یک سیستم مدیریتی و یک سیستم نرم‌افزاری در نظر بگیریم می‌توانیم به نتیجه قابل‌درکی در خصوص شناسایی شاخص‌های کلیدی مؤثر دست پیدا کنیم. با توجه به تحقیقات کتابخانه‌ای، شاخص‌های کلیدی پیاده‌سازی موفق سیستم مدیریت امنیت اطلاعت به این شرح به‌دست آمد: (۱) اراده، تعهد، مشارکت و پشتیبانی مدیریت ارشد، (۲) تعیین دامنه، نقشه راه، قلمرو و اهداف امنیتی از اجرا سیستم، (۳) ارتباطات و آگاهی کارکنان، (۴) آموزش و ارتقای سطح تخصص کارکنان، (۵) ایجاد فرهنگ امنیتی در سازمان و توسعه کار تیمی، (۶) مدیریت تغییر، (۷) تدارک منابع کافی (مالی و نیروی انسانی)، (۸) شناسایی دارایی و ریسک موجود، تحلیل، ارزیابی دقیق و به‌کارگیری کنترل مناسب، (۹) مدیریت پروژه قوی، (۱۰) ممیزی داخلی، (۱۱) به‌کارگیری مدیریت تداوم سرویس‌های ICT قبل از ISMS و (۱۲) الگوبرداری مناسب.

عوامل کلیدی موفقیت به دو دسته تقسیم شدند: (۱) عوامل کلیدی موفقیت در پیاده‌سازی سیستم‌های جامع سازمانی و (۲) عوامل کلیدی موفقیت در پیاده‌سازی سیستم‌های اطلاعاتی

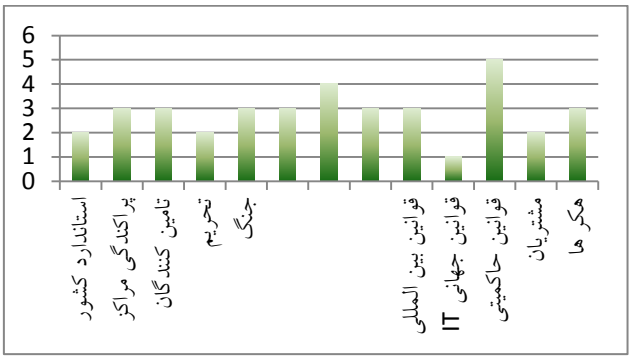
با جمع‌آوری و جمع‌بندی نظرات خبرگان، شاخص‌های کلیدی در پیاده‌سازی سیستم‌های اطلاعاتی به این شرح استخراج شد: (۱) کسب حمایت مدیر ارشد سازمان، (۲) آموزش و اطلاع‌رسانی مستمر به کارکنان، (۳) تأمین منابع مالی، (۴) به‌کارگیری تجربیان قبلی سازمان در خصوص پیاده‌سازی سایر استانداردهای مدیریتی معتبر، (۵) سیاست‌های امنیتی متناسب با دارایی‌ها، (۶) مشارکت و همکاری کارکنان، (۷) تدوین خط‌مشی و دستورالعمل‌ها بر اساس واقعیت سازمان، (۸) ممیزی مستمر داخلی و ارائه گزارش به مدیریت ارشد، (۹) مدیریت و پایش پروژه منطبق بر استاندارد مدیریت پروژه، (۱۰) به‌کارگیری نظام ارزیابی و پاداش عملکرد کارکنان حین پیاده‌سازی سیستم (۱۱) تعیین دقیق شاخص‌های اثربخشی سیستم و اندازه‌گیری و تحلیل مستمر آنها، (۱۲) انتخاب و به‌کارگیری مشاور توانمند در پیاده‌سازی، (۱۳) انطباق و همسویی کامل با سایر پروژه‌ها و طرح‌های فاوا، (۱۴) توان و کیفیت نظارتی کارفرما، (۱۵) تحلیل شکاف مناسب قبل از پیاده‌سازی استاندارد، (۱۶) تعیین دقیق دامنه و محدوده پروژه، (۱۷) انجام ارزیابی ریسک دارایی‌ها بر اساس تهدیدات و آسیب پذیرهای واقعی، (۱۸) نظام پذیرش سیستم، (۱۹) شرایط سیاسی و (۲۰) تحریم‌ها.

در ادامه نسبت به شناسایی و تحلیل تهدیدات موجود حول محور امنیتی در سازمان‌های حاکمیتی اقدام شد. علی‌رغم ارتباط تنگاتنگ بین سه مقوله استمرار کسب‌وکار، مدیریت بحران و پدافند غیرعامل، باید توجه داشت که از اهیت متفاوتی برخوردار هستند. اولین چیزی که برای سازمان‌ها مهم است استمرار کسب‌وکار است که می‌تواند بر اساس عوامل طبیعی و غیرطبیعی اتفاق بیفتد، سپس مسئله مدیریت بحران اهمیت دارد. مدیریت بحران همیشه

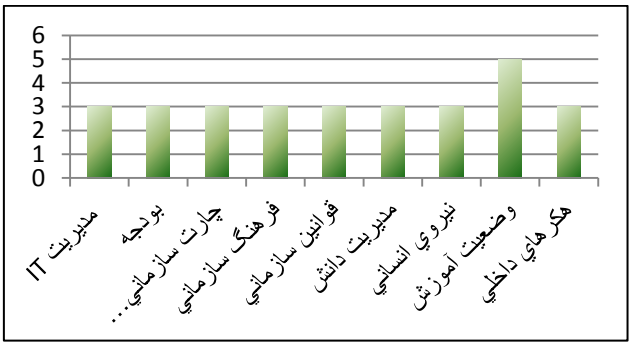
بعد از وقوع اتفاق است و منظور از اتفاقات در آن، اتفاقات تهاجمی نیست بلکه منظور اتفاقات طبیعی است. در مدیریت بحران برای فاجعه‌های طبیعی باید برنامه داشته باشیم تا در صورت وقوع، چگونگی بازیابی مشخص باشد. بحران‌ها موضوعاتی هستند ک اتفاق می‌افتند و نمی‌توان مانع از وقوع آنها شد و ساخته دست بشر نیستند. رتبهٔ آخر متعلق به پدافند غیرعامل است، که انواع اقدامات در رابطه با پیشگیری از تهدید دشمن را در بر می‌گیرد. پدافند غیرعامل مجموعه‌ای از برنامه‌ریزی‌ها، طراحی‌ها و اقداماتی است که باعث کاهش آسیب‌پذیری در مقابل تهدیدات دشمن می‌شود و از آن تحت عنوان بازدارندگی نیز یاد می‌شود. در پدافند سعی می‌شود از وقوع اتفاق جلوگیری شود. هر یک از این سه فرآیند چرخه‌های حیات، مدیریت‌های ریسک، کنترل‌ها، راهکارها و طریقه‌های بازبینی مختص به خود را دارند و برای هر کدام باید مدیریت وساختار تشکیلاتی متفاوتی وجود داشته باشد.

در زمینه شناخت تهدیدات موجود علاوه بر بررسی میدانی و اکتشاف مواردی که تأثیر در ایجاد امنیت دارد از خبرگان و صاحب نظرات امنیتی کمک گرفته شد و ۱۱۶ عامل در سه گروه کلی "عوامل بیرونی یا محیطی"، عوامل سازمانی یا درونی" و "عوامل فناوری و تکنولوژی" در جداول مربوطه دسته‌بندی شد. در هر گروه با بررسی‌های به عمل‌آمده نوع عمل تأثیرگذار در تحقیق کشف و از طریق آنها مجموعه عوامل که موجب تهدیدات می‌شوند گردآوری شد و کنترل هر یک به این صورت دسته‌بندی شد: (۱) مجموعه تهدیداتی که قابل‌کنترل می‌باشند، (۲) مجموعه تهدیداتی که کنترل‌پذیری دشوار و سختی دارند و (۳) مجموعه تهدیدات غیرقابل‌کنترل که در این تحقیق به عنوان پیش‌فرض در نظر گرفته شد.

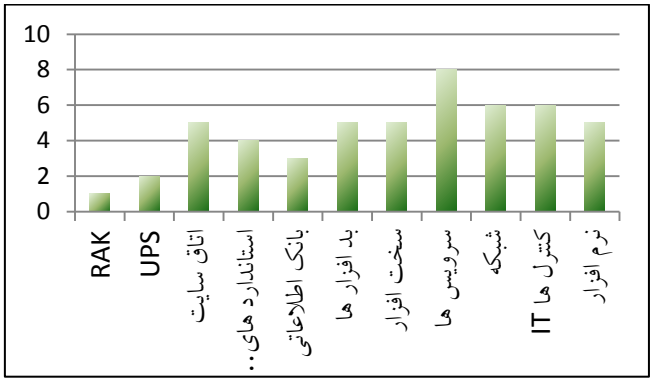
بر ای پیاده‌سازی سیستم ISMS در سازمان‌ها، شناخت تهدیدات در کنار دارایی‌ها کیفیت و عمق نگرش ما را ارتقا می‌بخشد. هرچند ممکن است نسبت به وجود این تهدیدات در دور اول یا بالاتر انجام چرخه دیمینگ کنترل خاصی اعمال نشود و براساس استراتژی برخورد با ریسک به عنوان پذیرش ریسک نام برده شود، اما در ذهن مدیر امنیت، تیم امنیت، تیم CERT و کارکنان درگیر پروژه وجود این تهدیدات مورد سئوال قرار گرفته و در تصمیمات به عنوان یک تهدید دائمی آورده می‌شود. مطالب و موارد یادشده در قالب نمودارهای مختلف تهیه و به صورت زیر ارائه شد.



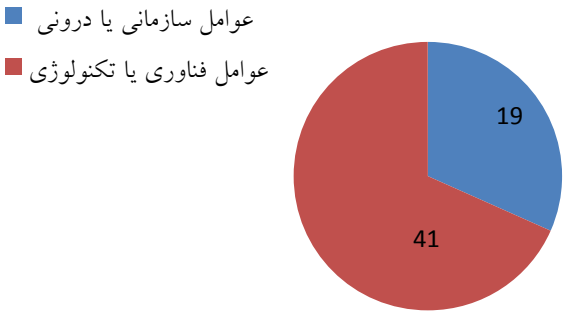
نمودار (۱): نوع عوامل در گروه محیطی



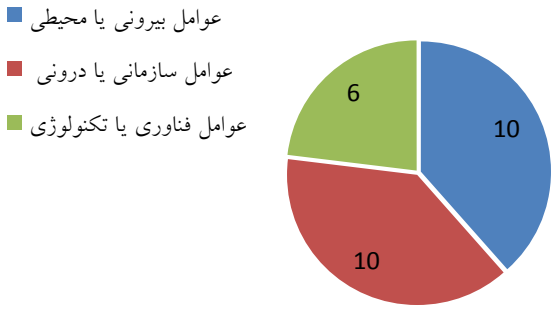
نمودار (۲): نوع عوامل در گروه سازمانی



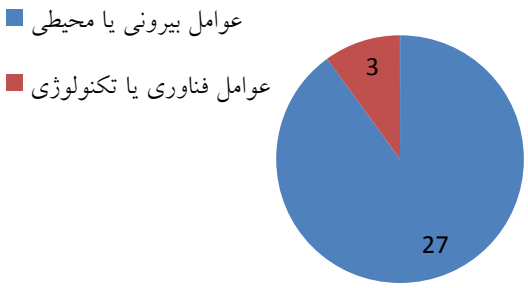
نمودار (۳): نوع عوامل در گروه فناوری و تکنولوژی



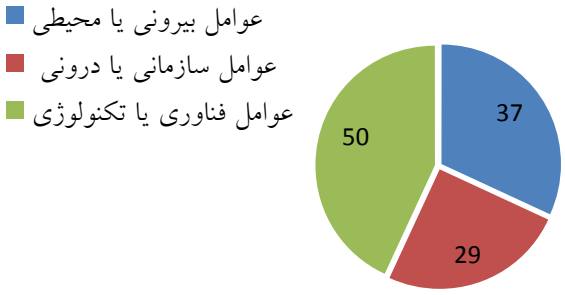
نمودار (٤): فراوانی عوامل کنترل شونده در گروه



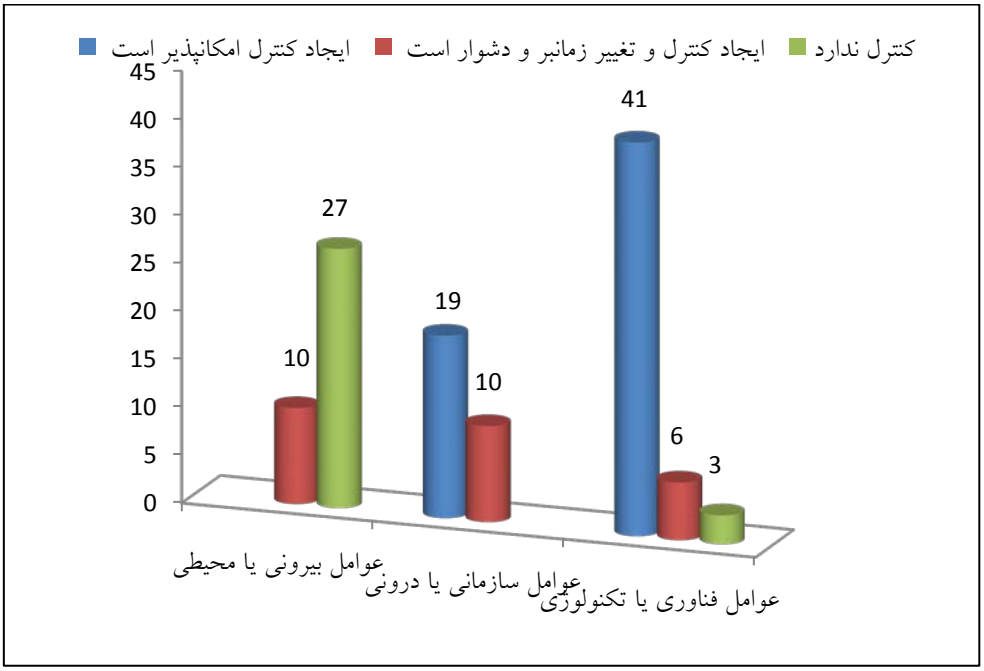
نمودار (٥): فراوانی عوامل با کنترل دشوار در گروه



نمودار (٦): فراوانی عوامل بدون کنترل در گروه



نمودار (۷): فراوانی عوامل در گروه‌ها در یک نگاه



نمودار (۸): گروه‌ها - نوع عوامل ـ عوامل

۳-۳- عوامل کلیدی موثر در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان‌های حاکمیتی بر اساس تهدیدات موجود

با توجه به مطالعات صورت گرفته و تحقیقات میدانی انجام شده شاخص‌های شناسایی شده در هر سطح پالایش شد و با توجه به نوع تهدیدات موجود طبقه‌بندی و به صورت جدول (۳)، (۴) و (۵) ارائه شد.

وضعیت سیستم‌های موروثی و زیرساخت فناوری اطلاعات (پیچیدگی سیستم‌های موجود و امکانات شبکه)
تیم های امنیتی و فنی پاسخگو (CERT)
نظام پذیرش سیستم (استاندارد فاوا)
به‌کارگیری مدیریت تداوم سرویس های ICT قبل ازISMS
انطباق و همسویی کامل با سایر پروژه‌ها و طرح‌های فاوا
خط مشی، سیاست‌های امنیتی و اجرایی
ممیزی و تحلیل اندازه‌گیری
توان و کیفیت نظارتی کارفرما
ارتقاء سطح آموزش، تخصص و مهارت کارکنان
بکار گیری تجربیان قبلی
تعیین دامنه و قلمرو پیاده‌سازی سیستم
تحلیل شکاف مناسب قبل از پیاده‌سازی استاندارد
برآورد و ارزیابی ریسک دارایی‌ها
به‌کارگیری سیستم های نرم‌افزاری و سخت‌افزاری مرتبط با ISMS
مدیریت داده‌ها و اطلاعات موجود

جدول (۳) عوامل فناوری تکنولوژی

فرهنگ‌سازمانی
باورهای مشترک
مدیریت تغییر
مدیریت منابع مالی و انسانی
نظام ایجاد انگیزش
اهداف شفاف
ارتباطات و آگاهی
مشارکت سازنده کارکنان
مدیریت پروژه
رسمیت
نقش مدیریت ارشد در پیاده‌سازی سیستم
تمرکزگرایی
مدیریت دانش

جدول (٤): عوامل درون‌سازمانی

الگوبرداری
تحریم‌ها
شرایط سیاسی
مشاور، مجری و پیمانکاران

جدول (٥): عوامل برون‌سازمانی

۳-٤- تعیین نمونه آماری

اگر بخواهیم حجم نمونه شکاف جمعیتی ۰/۵ یعنی نیمی از جمعیت حائز صفتی معین باشند. نیمی دیگر فاقد آن خواهد بود. معمولاً p و q را ۰/۵ در نظر می‌گیریم. مقدار z معمولاً ۱/۹۶ است. d می‌تواند ۰/۰۱ یا ۰/۰۵ باشد. در برخی از تحقیقات برای تصحیح حجم نمونه از فرمول تصحیح کوکران استفاده می‌شود. ساده‌شده فرمول به صورت فرمول (۱) می‌باشد.

فرمول (۱)

$$n = \frac{\frac{z^2 pq}{d^2}}{1+\frac{1}{N}\left(\frac{z^2 pq}{d^2}-1\right)}$$

وقتی‌که واریانس جامعه و احتمال موفقیت یا عدم موفقیت متغیر امشخص و روشن نباشد و نتوان از فرمول‌های آماری برای برآورد حجم نمونه استفاده کرد از جدول مورگان استفاده می‌شود. این جدول حداکثر تعداد نمونه را می‌دهد. (S: حجم نمونه، N: حجم جامعه است). با توجه به این توضیحات برای تعیین تعداد نمونه آماری در این تحقیق از روش کوکران با جامعه آماری محدود (۱۸۷عدد) استفاده شد که حجم نمونه برابر با عدد ۱۲۵.۹۹۶۰۷۱۲۷۸ گردید که این عدد به عدد ۱۲۶ گرد شد و این تعداد پرسشنامه پس از جمع‌آوری در تجزیه و تحلیل‌های آماری مورد استفاده قرار گرفت. با توجه به توضیحات فوق برای تعیین تعداد نمونه آماری در این تحقیق از روش کوکران با جامعه آماری محدود (۱۸۷عدد) استفاده گردید که حجم نمونه برابر شد با عدد ۱۲۵.۹۹۶۰۷۱۲۷۸ که این عدد را به عدد ۱۲۶ گرد کرده و این تعداد پرسشنامه را پس از جمع‌آوری در تجزیه و تحلیل‌های آماری مورد استفاده قرار گرفت .

۳-۵- متغیرهای مستقل و وابسته تحقیق

با توجه به موضوع تحقیق، بررسی تأثیر تمامی عوامل کلیدی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات، کاری بس دشوار و زمان‌بر می‌باشد. زیرا از یک‌سو، مستلزم تعیین معیارها و شاخص‌های متعددی است که باید مورد تأیید خبرگان و متخصصین قرار گیرد و از سوی دیگر بررسی پاسخ‌های اعضای جامعه آماری به سؤالات پرسشنامه، تحلیل آماری پیچیده و چندگانه‌ای خواهد داشت.

۳-۵-۱- متغیرهای مستقل تحقیق

در بررسی‌ها و نتایج به‌دست آمده تعداد ۳۲ عامل موثر در پیاده‌سازی سیستم‌ها از جمله سیستم مدیریت امنیت اطلاعات به عنوان متغیرهای مستقل در نظر گرفته شد. جدول (۶) متغیرهای مستقل پژوهش را نشان می‌دهد.

ردیف	متغیرهای مستقل	منابع	پرسشنامه
۱	وضعیت سیستم‌های موروثی و زیرساخت فناوری اطلاعات (پیچیدگی سیستم‌های موجود و امکانات شبکه)	[26] ، کورنگی، سجادیه	Q1
۲	تیم‌های امنیتی و فنی پاسخگو (CERT)	[26].[64],[35],[22],[37],[38],[43],[21],[14]	Q2
۳	نظام پذیرش سیستم (استاندارد فاوا)	کورنگی (شرکت علمی غرب آسیا)	Q3
۴	به‌کارگیری مدیریت تداوم سرویس‌های ICT قبل از ISMS	[۲۱][۱۲]	Q4
۵	انطباق و همسویی کامل با سایر پروژه‌ها و طرح‌های فاوا	کورنگی (شرکت علمی غرب آسیا)، سجادیه (شرکت پردازشگران داده آرا سپاهان)	Q5
۶	خط مشی، سیاست‌های امنیتی و اجرایی	[23],[26] منافی – خراسانی – ایزدی	Q6
۷	ممیزی و تحلیل اندازه‌گیری	Zwass 1988[23],[26],[27][14]	Q7
۸	توان و کیفیت نظارتی کارفرما	کورنگی – سجادیه	Q8
۹	ارتقاء سطح آموزش، تخصص و مهارت کارکنان	[23],steers1977,shanks et al.2000,Zwass1988,[14],[22],[26][27]	Q9
۱۰	بکار گیری تجربیان قبلی	سجادیه ، شاهینی، کورنگی، ایزدی	Q10
۱۱	تعیین دامنه و قلمرو پیاده‌سازی سیستم	[14],[21],[27],[25],[22],[40]	Q11
۱۲	تحلیل شکاف مناسب قبل از پیاده‌سازی استاندارد	کورنگی – سجادیه – ایزدی	Q12
۱۳	برآورد و ارزیابی رسیک دارایی‌ها	کورنگی – سجادیه – ایزدی ,[14]	Q13
۱۴	به‌کارگیری سیستم های نرم‌افزاری و سخت‌افزاری مرتبط با ISMS	کورنگی ، ایزدی، منافی	Q14
۱۵	مدیریت داده‌ها و اطلاعات موجود	[11],[10],[9],[26]	Q15
۱۶	فرهنگ‌سازمانی	[35],[26],[22]	Q16
۱۷	باورهای مشترک	[26],[60]	Q17
۱۸	مدیریت تغییر	[23],[26],[21],[34],[33] جوران و گاردفری ۲۰۰۰ و بالزاووا ۲۰۰۴	Q18
۱۹	مدیریت منابع مالی و انسانی	[25][21],[26] اینتر ولاکر – منافی – کورنگی – شاهینی	Q19
۲۰	نظام ایجاد انگیزش	[23],[25],[22]	Q20
۲۱	اهداف شفاف	[21],[14],[23],[26]	Q21
۲۲	ارتباطات و آگاهی	[22],[26],[21]	Q22
۲۳	مشارکت سازنده کارکنان	[23] گورنگی ، ایزدی ، سجادیه	Q23
۲۴	مدیریت پروژه	[37],[23],[26],[21]	Q24
۲۵	رسمیت	[23]steers1988	Q25
۲۶	نقش مدیریت ارشد در پیاده‌سازی سیستم	[21],[14],[15],[26],[40],[23]	Q26
۲۷	تمرکز گرایی	[26],[63]	Q27
۲۸	مدیریت دانش	[27],[22],[26]	Q28
۲۹	الگوبرداری	[21],[39][40],[64],[65]	Q29
۳۰	تحریم ها	کورنگی ، ایزدی، سجادیه، خراسانی	Q30
۳۱	شرایط سیاسی	کورنگی ، منافی	Q31,Q33
۳۲	مشاور، مجری و پیمانکاران	سجادیه ، کورنگی ، ایزدی ، [22]	Q32

جدول (٦): متغیر های مستقل

۳-۵-۲- متغیر وابسته تحقیق

متغیر وابسته این تحقیق "پیاده‌سازی و اجرای موفق سیستم مدیریت امنیت اطلاعات" می‌باشد که در اثر اجرای موفقیت سیستم، سطح امنیت اطلاعات با به‌کارگیری کنترل‌های حوزه ISMS افزایش می‌یابد. امنیت، حاصل افزاش مؤلفه‌های محرمانگی ، یکپارچگی و دسترس‌پذیری اطلاعات می‌باشد.

۳- ٦- روش‌های آماری

تجزیه و تحلیل اطلاعات آماری این تحقیق با استفاده از نرم‌افزار SPSS 21, SPSS16, LISREL8.5 انجام می‌شود. آزمون‌های آماری صورت گرفته در انجام این تحقیق شامل: (۱) آزمون کولموگروف – اسمیرنوف برای نرمال بودن داده‌های جمع‌آوری شده، (۲) آزمون تحلیل عاملی تأییدی به منظور بررسی روایی سازه، (۳) آزمون T تک جمله‌ای به منظور پاسخ به سئوالات اصلی تحقیق و رتبه‌بندی شاخص‌های کلیدی، (۴) آزمون فریدمن به منظور پاسخ به سئوالات اصلی تحقیق و رتبه‌بندی عوامل کلیدی، (۵) آزمون T تک نمونه‌ای به منظور اثبات فرضیه اول و (۶) آزمون رگرسیون جهت اثبات فرضیه دوم و ارائه مدل می‌باشد.

۳-۷- بحث و تحلیل

در پژوهش حاضر شناسایی شاخص‌های کلیدی موفقیت طی مراحل مختلف تحلیل شد. (۱) از بین ۶۴ شاخص شناسایی‌شده ۳۲ شاخص از طریق مطالعه، مصاحبه با خبرگان و تحلیل پژوهشگر، به عنوان شاخص‌های کلیدی تحقیق تعیین شد، (۲) سئوالات به گونه‌ای طراحی شدند که اثربخشی شاخص‌های موجود را مورد سنجش قرار دهند و با انجام تست‌های اولیه و تأیید پایایی سازه پرسشنامه، اعتبار شاخص‌های مذکور تأیید شد، (۳) با انجام آزمون بارتلت و شاخص KMO میزان همبستگی هر شاخص با عامل مرتبط و اثربخشی ایجادشده (متغیر وابسته) تاحدودی مشخص شد. از آنجا که مقدار شاخص KMO برابر است با ۰/۷۳۹، بیشتر از ۰/۶ است تعداد نمونه (در اینجا همان تعداد پاسخ‌دهندگان) برای تحلیل عاملی کافی تشخیص داده شد. همچنین مقدار معناداری (Sig) آزمون بارتلت برابر ۰/۰۰۰، یعنی کوچک‌تر از ۵ درصد شد که نشان می‌دهد تحلیل عاملی برای شناسایی ساختار مدل عاملی، مناسب است، (۴) انجام آزمون‌های فوق این نتیجه را در پی داشت که مقدار به‌دست آمده برای هر کدام از سؤالات نشان‌دهنده ضریب همبستگی می‌باشد که هر ستونی که مقدار بیشتری داشته باشد نشان‌دهنده این است که شاخص با متغیر مذکور ارتباط دارد، برای مثال شاخص اول در ستون اول با مقدار ۰/۴۴۷ با دیدگاه فناوری در موفقیت پیاده‌سازی سیستم مدیریت اطلاعات ارتباط دارد، (۵) نتایج تحلیل‌های عاملی نشان داد که تمام ۳۲ شاخص یادشده شامل شاخص‌های فناوری و تکنولوژی، سازمانی (درون‌سازمانی و برون‌سازمانی) در اثربخشی و موفقیت پیاده‌سازی ISMS ، با مقادیر تی (بیشتر از ۱/۹۶) و بار عاملی (بیشتر از ۰/۴) مورد قبولی برخوردار می‌باشند و برای موفقیت پیاده‌سازی ISMS شاخص‌های مناسبی محسوب می‌شوند، (۶) با توجه به نتایج آزمون تی تک نمونه‌ای می‌توان گفت شاخص‌هایی که دارای میانگین بیشتر از ۳ و آماره تی بیشتر از ۱/۹۶ و سطح معناداری (sig) کمتر از ۰/۰۵ باشد به عنوان شاخص‌های کلیدی موثر در اجرا و پیاده‌سازی موفق سیستم مدیریت امنیت اطلاعات (ISMS) شناخته می‌شوند، (۷) با توجه به تحلیل فوق نشان داده شد که تمامی شاخص‌های مورد سنجش ارتباط تنگاتنگی با موضوع دارند و می‌توان ۳۲ مورد شاخص ارائه‌شده در مدل مفهومی را به عنوان شاخص کلیدی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات به حساب آورد. البته می‌توان این‌گونه نیز نتیجه‌گیری کرد که تمامی شاخص‌هایی که میانگین بالاتر از ۳ و تی بالاتر از ۱/۹۶ دارند به طور بالقوه شاخص‌های کلیدی برای موفقیت می‌باشند و سازمان مذکور در پیاده‌سازی سیستم مدیریت امنیت اطلاعات مورد توجه قرار داده است. و آنهایی که میانگین و آماره کمتری به دست آورده‌اند به دلیل فقدان موجودیت و عدم تمرکز و توجه سازمان، موجب عدم قطعیت موفقیت در متغیر وابسته شده‌اند. لذا می‌توان از آنها به عنوان شاخص‌های کلیدی‌ای که سازمان نسبت به آن توجه لازم نداشته است. یادکرد.

بنابراین ایجاد و بهره‌گیری شاخص‌های فراموش‌شده در کنار تقویت شاخص‌های اثبات‌شده متناسب با میانگین و آماره کسب‌شده در آزمون تی تک نمونه‌ای موجب ارتقای سطح پیاده‌سازی سیستم می‌شوند. از آنجا که سئوالات ۳۱ و ۳۳ در رابطه با یک موضوع مطرح شده‌اند بنابراین میانگین آنها با عدد ۲/۶۳ به عنوان شاخصی تأثیرگذار می‌تواند محسوب شود. اما در خصوص سئوال ۳۰ با توجه به طرح سئوال به صورت معکوس می‌توان نتیجه گرفت که میانگین و آماره عکس آن بالاتر از ۳ و ۱/۹۶ بوده و به عنوان شاخص کلیدی فراموش‌شده نیست.

آسایش	ایده آل	هشدار	اضطرار	بحران
	این شاخص کلیدی جزء شاخص‌هایی است که سازمان به آن توجه خوبی داشته است. تمرکز و نگهداری آن در سطح مربوطه اقدام مفید سازمان است.	این شاخص کلیدی جزء شاخص‌هایی است که سازمان به صورت متوسط به آن در هنگام اجرای سیستم توجه داشته است. لذا تقویت آن تا پیاده‌سازی موفق الزامی است.	این شاخص کلیدی جزء شاخص‌های فراموش‌شده در سازمان است و باید نسبت به ایجاد و بهره‌گیری از آن با قید فوریت جهت پیاده‌سازی موفق سیستم اقدام گردد	

جدول (۷): وضعیت شاخص‌ها و عکس‌العمل پیشنهادی سازمان

ردیف	شاخص کلیدی	Q	میانگین	آماره	sig	نوع عکس‌العمل سازمان
۱	وضعیت سیستم‌های موروثی و زیرساخت فناوری اطلاعات (پیچیدگی سیستم‌های موجود و امکانات شبکه)	Q1	3.42	6.108	.000	هشدار
۲	تیم های امنیتی و فنی پاسخگو (CERT)	Q2	3.57	6.523	.000	هشدار
۳	نظام پذیرش سیستم (استاندارد فاوا)	Q3	3.49	7.203	.000	هشدار
۴	به‌کارگیری مدیریت تداوم سرویس های ICT قبل ازISMS	Q4	2.84	-1.742	.084	اضطرار
۵	انطباق و همسویی کامل با سایر پروژه‌ها و طرح های فاوا	Q5	3.35	3.834	.000	هشدار
۶	خط مشی، سیاست‌های امنیتی و اجرایی	Q6	3.56	6.227	.000	هشدار
۷	ممیزی و تحلیل اندازه‌گیری	Q7	4.02	12.503	000	ایده آل
۸	توان و کیفیت نظارتی کارفرما	Q8	3.79	10.701	.000	هشدار
۹	ارتقاء سطح آموزش، تخصص و مهارت کارکنان	Q9	3.29	2.802	.006	هشدار
۱۰	بکار گیری تجربیان قبلی	Q10	3.40	5.229	.000	هشدار
۱۱	تعیین دامنه و قلمرو پیاده‌سازی سیستم	Q11	3.56	5.828	.000	هشدار
۱۲	تحلیل شکاف مناسب قبل از پیاده‌سازی استاندارد	Q12	3.50	6.052	.000	هشدار
۱۳	برآورد و ارزیابی ریسک دارایی‌ها	Q13	3.32	3.710	.000	هشدار
۱۴	به‌کارگیری سیستم‌های نرم‌افزاری و سخت‌افزاری مرتبط با ISMS	Q14	2.82	-1.853	.066	اضطرار
۱۵	مدیریت داده‌ها و اطلاعات موجود	Q15	3.75	9.218	.000	هشدار
۱۶	فرهنگ‌سازمانی	Q16	3.49	5.797	.000	هشدار
۱۷	باورهای مشترک	Q17	3.50	6.109	000	هشدار
۱۸	مدیریت تغییر	Q18	3.41	5.218	.000	هشدار
۱۹	مدیریت منابع مالی و انسانی	Q19	3.29	3.839	.000	هشدار
۲۰	نظام ایجاد انگیزش	Q20	2.35	-5.978	.000	اضطرار
۲۱	اهداف شفاف	Q21	2.92	-.876	.383	اضطرار
۲۲	ارتباطات و آگاهی	Q22	3.25	2.987	.003	هشدار
۲۳	مشارکت سازنده کارکنان	Q23	3.60	6.305	.000	هشدار
۲۴	مدیریت پروژه	Q24	3.45	4.648	.000	هشدار
۲۵	رسمیت	Q25	3.49	5.051	.000	هشدار
۲۶	نقش مدیریت ارشد در پیاده‌سازی سیستم	Q26	3.53	6.267	.000	هشدار
۲۷	تمرکزگرایی	Q27	3.46	5.797	.000	هشدار
۲۸	مدیریت دانش	Q28	3.14	1.896	.060	هشدار
۲۹	الگوبرداری	Q29	3.09	.946	.346	هشدار
۳۰	تحریم‌ها	Q30	2.53	-5.051	.000	هشدار
۳۱	شرایط سیاسی	Q31,Q33	۲.۶۳	-۴.۲۱۱	.000	اضطرار
۳۲	مشاور، مجری و پیمانکاران	Q32	3.27	2.561	.012	هشدار

جدول (۸): وضعیت شاخص‌ها و عکس‌العمل پیشنهادی سازمان

به منظور رتبه‌بندی اولویت هریک از عوامل کلیدی موثر در اجرا و پیاده‌سازی سیستم مدیریت امنیت اطلاعات از رتبه‌بندی فرید من استفاده شد شود که نتایج مندرج در جدول (۹) به دست آمد.

متغیرهای مستقل	رتبه میانگین	رتبه
عوامل فناوری و تکنولوژی	۲/۴۶	۱
عوامل سازمانی یا درونی	۲/۲۱	۲
عوامل خارجی برون‌سازمانی	۱/۳۳	۳

جدول (۹): رتبه‌بندی عوامل موفقیت در پیاده‌سازی سیستم مدیریت امنت اطلاعات

با توجه به نتایج به دست آمده از میانگین می‌توان گفت که عوامل فناوری و تکنولوژی‌ها با میانگین ۲/۴۶ دارای بالاترین رتبه و عوامل سازمانی یا درونی با میانگین ۱/۳۳ دارای پایین‌ترین رتبه می‌باشد. جدول آزمون فریدمن در خصوص رتبه‌بندی عوامل موفقیت در پیاده‌سازی سیستم مدیریت امنیت اطلاعات به شرح جدول (۱۰) می‌باشد.

N	۱۲۶
Chi-square	۹۰/۵۸۰
Df	۲
Sig	۰/۰۰۰

جدول (۱۰): آزمون فریدمن در خصوص رتبه‌بندی عوامل

از آنجا که sig (سطح معناداری) کمتر از ۰/۵ است، ادعای یکسان بودن رتبه (اولویت) هر یک از عوامل کلیدی موثر در اجرا و پیاده‌سازی سیستم مدیریت امنیت اطلاعات پذیرفته نمی‌شود.

متغیر پیش بین	ضریب مسیر (β)	آماره t	ضریب تعیین کل (R^2)
عوامل فناوری و تکنولوژی	۰/۵۲۴	۵/۱۲**	۰/۵۲۹
عوامل سازمانی یا درونی	۰/۲۴۶	۲/۶۲**	
عوامل خارجی یا بیرونی	۰/۰۲	۰/۱۶۲	

** $p < 0.01$ * $p < 0.05$

جدول (۱۱): ضرایب مسیر، آماره t و ضریب تعیین (متغیر وابسته: ISMS)

با توجه به ضرایب مسیر و همچنین آماره می‌توان گفت عوامل فناوری و تکنولوژی و عوامل درون‌سازمانی در سطح اطمینان ۹۹٪ بر اجرا و پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) تأثیر معنادار و مثبت دارند. اما متغیر عوامل خارجی یا برون‌سازمانی تأثیر معناداری بر اجرا و پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) ندارد. همچنین با توجه به آزمون تی تک نمونه‌ای که برای اثبات فرضیه اول استفاده شد مشخص شد که عوامل موفقیت در پیاده‌سازی سیستم مدیریت امنیت اطلاعات به صورت یکسان تأثیر نداشته و دو عامل " فناوری و تکنولوژی" و "درون‌سازمانی" تأثیرشان بیشتر از عامل "برون‌سازمانی" است و به این ترتیب فرضیه دوم مبنی بر تأثیر متفاوت عوامل کلیدی موفقیت در پیاده‌سازی ISMS اثبات می‌شود.

معیار	میانگین	آماره t	Sig
عوامل فناوری و تکنولوژی	۳/۴۴	۸/۴۹	۰/۰۰۰
عوامل درون‌سازمانی	۳/۲۹	۵/۰۶	۰/۰۰۰
عوامل برون‌سازمانی	۲/۸۲	۱/۸۲	۰/۰۹۱

جدول (۱۲): نتایج آزمون t تک نمونه‌ای

از آنجا که sig عوامل فناوری و تکنولوژی و عوامل درون‌سازمانی کمتر از ۵٪ و مقدار آماره t بیشتر از ۱/۹۶ است پس فرض H_1 آن رد نمی‌شود. عوامل فناوری و تکنولوژی و عوامل درون‌سازمانی به عنوان عوامل کلیدی در پیاده‌سازی و اجرای مستمر سیستم مدیریت امنیت اطلاعات موثر می‌باشند.

از آنجائیکه sig عوامل برون‌سازمانی بیشتر از ۵٪ و مقدار آماره t کمتر از ۱/۹۶ است پس فرض H_0 آن رد نمی‌شود. عوامل برون‌سازمانی به عنوان عوامل کلیدی در پیاده‌سازی و اجرای مستمر سیستم مدیریت امنیت اطلاعات موثر نمی‌باشد.

نام شاخص	Question	رتبه میانگین	رتبه‌بندی شاخص PMO
ممیزی و تحلیل اندازه‌گیری	Q7	24.59	1
توان و کیفیت نظارتی کارفرما	Q8	22.3	2
مدیریت داده‌ها و اطلاعات موجود	Q15	21.42	3
خط مشی، سیاست‌های امنیتی و اجرایی	Q6	20.11	4
ممیزی و تحلیل اندازه‌گیری	Q7	19.86	5
توان و کیفیت نظارتی کارفرما	Q8	19.79	6
مشارکت سازنده کارکنان	Q23	19.5	7
نقش مدیریت ارشد در پیاده‌سازی سیستم	Q26	19.06	8
فرهنگ‌سازمانی	Q16	18.99	9
باورهای مشترک	Q17	18.94	10
تحلیل شکاف مناسب قبل از پیاده‌سازی استاندارد	Q12	18.73	11
نظام پذیرش سیستم (استاندارد فاوا)	Q3	18.62	12
رسمیت	Q25	18.5	13
مدیریت پروژه	Q24	18.32	14
تمرکزگرایی	Q27	18.21	15
وضعیت سیستم‌های موروثی و زیرساخت فناوری اطلاعات (پیچیدگی سیستم‌های موجود و امکانات شبکه)	Q1	18.19	16
بکار گیری تجربیان قبلی	Q10	18.09	17
ارتقاء سطح آموزش، تخصص و مهارت کارکنان	Q9	17.58	18
مدیریت تغییر	Q18	17.57	19
انطباق و همسویی کامل با سایر پروژه‌ها و طرح های فاوا	Q5	17.32	20
مشاور، مجری و پیمانکاران	Q32	17.23	21
برآورد و ارزیابی ریسک دارایی‌ها	Q13	17.11	22
ارتباطات و آگاهی	Q22	16.19	23
مدیریت منابع مالی و انسانی	Q19	16.14	24
الگوبرداری	Q29	14.92	25

مدیریت دانش	Q28	14.89	26
اهداف شفاف	Q21	13.02	27
به‌کارگیری مدیریت تداوم سرویس های ICT قبل ازISMS	Q4	12.81	28
به‌کارگیری سیستم‌های نرم‌افزاری و سخت‌افزاری مرتبط با ISMS	Q14	12.47	29
شرایط سیاسی	Q31,Q33	10.69	30
تحریم‌ها	Q30	9.64	31
نظام ایجاد انگیزش	Q۲۰	9.52	32

جدول (۱۳): جدول رتبه‌بندی شاخص‌های کلیدی موفقیت در پیاده‌سازی سیستم مدیریت امنیت اطلاعات

٤- نتیجه گیری کلی

نتایج این پژوهش را می‌توان به صورت زیر جمع‌بندی کرد: (۱) انجام این تحقیق هنگامی‌که سازمان مورد مطالعه در نیمه راه پیاده‌سازی سیستم مدیریت امنیت اطلاعات بود، موجب ایجاد انرژی و هم‌افزایی مجدد در نوع نگرش به موضوع و ایجاد بسترها و توانایی‌های لازم جهت ادامه مسیر گردید، (۲) با توجه به اینکه در انجام تحقیق نظر کارشناسان مرتبط، مدیران امنیت و روسای ادارات مربوطه شنیده شد و در زمینه‌های مختلف و تحلیل مشکلات بحث و گفتگو انجام گرفت، پرسش و پاسخ های متوالی موجب ایجاد طوفان ذهنی در خصوص تفکر عمیق در رابطه با مشکلات موجود شد، (۳) فرصتی مهیا شد تا افراد ذیصلاح ترغیب به ارائه نظر و در نهایت تشکیل کمیته شبکه و امنیت در مجموعه سازمان بنادر و دریانوردی و بنادر تابعه شوند، (۴) شرایطی پدید آمد تا بنادری که در اجرای چرخه‌های دوم یا چندم امنیت بودند به صورت الگوی بنادری درآیند که در ابتدای راه بودند، (۵) با انجام این تحقیق سازمان مرکزی را متقاعد شد تا نسبت به برگزاری دوره‌های آموزشی مرتبط و بازآموزی موضوع سیستم امنیت اطلاعات اقدام نماید، (۶) با انجام این تحقیق سازمان مرکزی را متقاعد شد تا نسبت به برنامه‌ریزی و تخصیص رسانه و نرم‌افزاری جهت انجام امور مذکور اقدام نماید، (۷) نقطه نظرات مجریان طرح‌های امنیتی مراکز بزرگ و مشابه گرفته شد که می‌تواند به عنوان یکی از مراجع مورد استفاده سازمان‌های ذینفع قرار گیرد و (۸) در مباحث امنیت نقطه نظرات مدیران امنیت سازمان‌های دولتی اخذ و در بعضی از موارد به عنوان سئوال‌های چالش‌برانگیز به مخاطبان موضوع (مجریان و پیمانکاران) انتقال داده شد و اطلاع‌رسانی این مجموعه نظرات و تفکرات می‌تواند دستاورد مفیدی برای بخش خصوصی فعال در این حوزه باشد.

مراجع

۱. کلانتری، ۱۳۸۸داده های آماری در SPSS
۲. استاندارد ISMS از دکتر کامران رضایی مدیرعامل شرکت مشارکتی TUV NORD Iran
۳. استاندارد ISO/IEC 270001 :2005 ترجمه مهندس ایمان خراستنی راد ،حسن حسین آبادی ،رامین امین زاده
۴. کتاب بهبود روش‌ها و حیطه عملکرد آن‌ها – دکتر خدابخش داشگر زاده
۵. عوامل کلیدی موفقیت در پیاده‌سازی مدیریت فرآیند و ارائه چهارچوبی برای ارزیابی آمادگی سازمان.نشریه مدیریت صنعتی دوره یکم شماره سوم ۱۳۸۸
۶. عوامل کلیدی موفقیت مدیریت دانش به منظور افزایش خلاقیت و یادگیری سازمانی در شرکت فرودگاه‌های کشور محمدحسن بیگی (عنوان پایان‌نامه کارشناسی ارشد).
۷. ارائه یک متدولوژی برای تجمیع کاربردهای سازمانی با سبک معماری سرویس گرا (SOA).رحمان منفرد (عنوان پایان‌نامه کارشناسی ارشد).
۸. بررسی عوامل کلیدی موفقیت در پیاده‌سازی و استقرار سیستم جامعه بندری در سازمان بنادر و دریانوردی. سهیلا شیبانی مقدم (عنوان پایان‌نامه کارشناسی ارشد).
۹. خاکی، غلامرضا، ۱۳۸۲ ، روش تحقیق با رویکردی به پایان‌نامه نویسی، انتشارات بازتاب.
۱۰. دانایی‌فرد و الوانی و آذر، حسن و سید مهدی و عادل، ۱۳۸۷ ، روش‌شناسی پژوهش کمی در مدیریت :رویکردی جامع، انتشارات صفار - اشراقی.

۱۱. مدیریت تغییر برای اجرای فناوری اطلاعات–ماهنامه تدبیر–سال هفدهم–شماره ۱۶۷
۱۲. کتاب ۱۷ اصل کار تیمی . نویسنده: جان ماکسول مترجم: مهندس عزیز کیاوند ناشر: نشر فرانوبت چاپ: چاپ اول – پاییز ۱۳۸۲
۱۳. حمایت و پشتیبانی تمامی واحدهای سازمانی در پیشبرد موفقیت‌آمیز پروژه (یوسف و همکاران، ۲۰۰۴؛ ژانگ و همکاران، ۲۰۰۵)
۱۴. دانش و آگاهی مناسب قهرمان پروژه بر مسایل فنی و کسب‌وکار (سامرز و نلسون، ۲۰۰۱).
15. http://www.parsmodir.com/db/research/cochran.php
16. J. Laudon, K.C. Laudon , J.P. Laudan, “Management Information System :Managing the Digital Firm”, 2006