DOI: http://dx.doi.org/10.22059/jitm.2015.52454

مدیریت فناوری اطلاعات
دانشکدهٔ مدیریت دانشگاه تهران

دورهٔ ۶، شمارهٔ ۴
زمستان ۱۳۹۳
ص. ۵۶۶- ۵۵۱

رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف

امیرهوشنگ تاج‌فر[۱]، محمد محمودی میمند[۲]، فاطمه رضاسلطانی[۳]، پوریا رضاسلطانی[۴]

چکیده: امروزه، اطلاعات نقش سرمایهٔ یک سازمان را ایفا می‌کند و حفاظت از اطلاعات سازمان یکی از ارکان مهم بقای آن است. سیستم مدیریت امنیت اطلاعات (ISMS)، حفاظت از اطلاعات را در سه مفهوم خاص محرمانه‌بودن اطلاعات، صحت اطلاعات و در دسترس‌بودن اطلاعات تعریف می‌کند. بسیاری از شکست های پیاده سازی ISMS ریشه در مسائل سازمانی و بی‌توجهی به وضعیت آمادگی سازمان قبل از پیاده‌سازی دارد. در این پژوهش تلاش شده است موانع پیاده سازی ISMS برحسب میزان اهمیت، به روش تحلیل سلسله‌مراتبی رتبه بندی شود و میزان آمادگی سازمان در پیاده‌سازی ISMS به‌کمک ابزار پرسشنامه مشخص شود. پژوهش به روش توصیفی ـ پیمایشی انجام گرفته و از نظر هدف، کاربردی است. نتایج پژوهش مهم‌ترین مانع در راه پیاده‌سازی ISMS را ناهمخوانی ساختار سازمانی با نیازهای ISMS می‌داند و ترس کارکنان از سخت‌شدن فرایندهای کار با اجرای ISMS را کم‌اهمیت‌ترین مانع معرفی کرده است؛ ضمن آنکه میزان آمادگی مدیریت اکتشاف در پیاده‌سازی ISMS پایین‌تر از حد متوسط است.

واژه های کلیدی: ***تحلیل سلسله‌مراتبی، سنجش آمادگی، سیستم مدیریت امنیت اطلاعات، موانع پیاده‌سازی.***

۱. استادیار مدیریت فناوری اطلاعات، دانشگاه پیام نور، تهران، ایران
۲. دانشیار مدیریت اجرایی و MBA، دانشگاه پیام نور، تهران، ایران
۳. کارشناس‌ارشد مدیریت فناوری اطلاعات، دانشگاه پیام نور تهران غرب، ایران
۴. دانشجوی دکتری سنجش و اندازه‌گیری، دانشگاه تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۲/۱۲/۲۵
تاریخ پذیرش نهایی مقاله: ۱۳۹۳/۰۴/۱۰
نویسندهٔ مسئول مقاله: فاطمه رضاسلطانی
E-mail: ryma_rooz@yahoo.com

مقدمه

حیات سازمان‌ها ارتباط نزدیکی با سیستم‌های اطلاعاتی آنها دارد. سیستم‌های اطلاعاتی نیز همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در خدمات‌رسانی هستند. به‌منظور حل مسئلهٔ امنیت اطلاعات، سازمان نیازمند به‌کارگیری طیف گسترده‌ای از دانش، فناوری و قوانین سازمانی است و درعین حال باید مطمئن شد که سازمان فقط روی راه‌حل‌های فنی متمرکز نیست، بلکه اجزای کلیدی دیگر امنیت اطلاعات، شامل فرایندها و کارکنان نیز در آن لحاظ شده است (هونان، ۲۰۰۶ و کرمر، ۲۰۰۶).

در سال ۲۰۰۵ یکی از جامع‌ترین استانداردهای سیستم مدیریت امنیت اطلاعات[1] با نام ایزو ۲۰۰۵ :۲۷۰۰۱ (ISO/IEC) [2] تدوین شد. هدف از تدوین این استاندارد ملی، مشخص‌کردن الزامی برای ایجاد، اجرا، بهره‌برداری، پایش، بازنگری، نگهداری، بهبود و ارتقای یک سیستم مدیریت امنیت اطلاعات مستند شده، با در نظر گرفتن مفهوم ریسک‌های کلان کسب‌وکار سازمان بود. در تاریخ ۲۵ سپتامبر ۲۰۱۳، پیش‌نویس نسخهٔ جدید استاندارد ایزو ۲۷۰۰۱ با نام ایزو ۲۷۰۰۱: ۲۰۱۳ منتشر و جایگزین استاندارد قبلی، یعنی ایزو ۲۷۰۰۱: ۲۰۰۵ شد. در این استاندارد بر تعداد دامنه‌های کنترلی افزوده شد و از ۱۱ به ۱۴ رسید و تعداد کنترل‌ها از ۱۳۳ به ۱۱۳ کاهش یافت.

از ویژگی‌های این استاندارد وجود ۱۱۳ کنترل امنیتی در قالب ۳۵ هدف کنترلی و ۱۴ حوزه شامل خط‌مشی امنیتی، سازمان، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی و محیطی، امنیت عملیات، امنیت ارتباطات، کنترل دسترسی، رمزنگاری، ارتباط با تأمین‌کنندگان، اکتساب، توسعه و نگهداری سیستم‌های اطلاعاتی، مدیریت حوادث امنیت اطلاعات، مدیریت تداوم کسب‌وکار و انطباق است که جنبه‌های گوناگون مدیریتی، عملیاتی و فنی را در یک سازمان پوشش می‌دهد (سازمان استاندارد بین‌المللی، ۲۰۱۳).

با توجه به اهمیت این سیستم فنی ـ مدیریتی در کشور، طبق بخشنامهٔ شمارهٔ ۸۶-۱۳۷۱۱/ م / ۳۸۵۰۵ مورخ ۱۳۸۶/۸/۱۰معاون اول محترم رئیس جمهور، کلیهٔ دستگاه‌های دولتی و غیردولتی موظف به تهیهٔ طرح سیستم مدیریت امنیت اطلاعات شدند. از آنجا که طراحی و استقرار ISMS سرمایه‌گذاری نسبتاً زیادی را می‌طلبد، ارزیابی شرایط سازمان از حیث میزان آمادگی، امری ضروری به نظر می‌رسد (خراسانی راد، حسین‌آبادی و امیرزاده، ۱۳۷۵).

---

1. Information Security Management System (ISMS)
2. International Electrotechnical Commission/ International Standard Organization

برای سیستم مدیریت امنیت اطلاعات ویژگی‌های گوناگونی بیان شده است. برای مثال ذکرشده که باید مدیریت آن متمرکز باشد و واحد و فرایندهایی مجزا از سایر بخش‌های سازمانی (به‌ویژه بخش فناوری اطلاعات) داشته باشد؛ البته باید هماهنگی و هم راستایی میان قسمت‌های گوناگون نیز حفظ شود (ارنست جونز، ۲۰۰۶). همچنین تأکید شده است که رویکرد صحیح باید تکرارشونده، نظام‌مند، کامل، سازگار و آسان برای درک، تجزیه و تحلیل باشد (کوتونیا و سومرویل، ۱۹۹۸). ویژگی دیگر آنکه رویکرد مدیریت امنیت، باید تعادلی میان حفاظت اطلاعات و دسترسی مجاز باشد. نکتهٔ مهم این است که امنیت اطلاعات باید در تمام سطح سازمانی (راهبردی، تاکتیکی و عملیاتی) مدیریت شود و کنترل‌های لازم پیاده‌سازی شوند. همچنین بهتر است امنیت اطلاعات به‌صورت فرایندی مداوم اجرا شود و شناسایی، ارزیابی و پیاده‌سازی را برای همهٔ اجزا دربرگیرد (ریان، ۲۰۰۶). همچنین چارچوب مدیریت امنیت باید به‌گونه‌ای باشد که اجرایش آسان، کم‌هزینه و مناسب با نیازهای تجارت الکترونیکی باشد (زوکاتو، ۲۰۰۷).

هدف اصلی پژوهش، رتبه‌بندی موانع استقرار سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی پیاده سازی در مدیریت اکتشاف شرکت ملی نفت ایران است. فرضیه‌های پژوهش به‌شرح زیر تدوین شده‌اند:

۱. بین مؤلفه‌های موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات رتبه‌بندی وجود دارد؛
۲. میزان آمادگی مدیریت اکتشاف شرکت ملی نفت ایران در پیاده‌سازی سیستم مدیریت امنیت اطلاعات، بیشتر از حد متوسط است[۱]؛
۳. سطح همهٔ مؤلفه‌های آمادگی مدیریت اکتشاف شرکت ملی نفت ایران در پیاده‌سازی سیستم مدیریت امنیت اطلاعات، بیشتر از حد متوسط است؛
۴. بین میانگین مؤلفه های آمادگی مدیریت اکتشاف شرکت ملی نفت ایران در پیاده سازی سیستم مدیریت امنیت اطلاعات، تفاوت معنادار آماری وجود دارد.

با توجه به بررسی مبانی نظری و پیشینهٔ پژوهش، هشت مؤلفهٔ موانع مدیریتی، محیطی، فنی، آموزشی، اقتصادی، ساختاری، فردی و فرهنگی و ۲۵ زیرمؤلفهٔ آگاه‌نبودن مدیریت از ضرورت امنیت، بهره‌نبردن از حمایت کامل و مشارکت مدیریت ارشد، برخوردار نبودن از مدیریت زمانی و مالی پروژه، وجود نهادهای موازی در تصمیم‌گیری (فناوری اطلاعات و حراست)، بی‌توجهی به ISMS به‌منزلهٔ مزیت رقابتی، تعریف نادرست قلمرو استقرار ISMS، برخوردار نبودن از زیرساخت مناسب فناوری اطلاعات، نداشتن تخصص و تجربهٔ کافی شرکت‌های پیمانکار، بهره‌نبردن از مشاور برون‌سازمانی، تدوین نامناسب خط‌مشی امنیت اطلاعات، کیفیت پایین

---

۱. بر اساس طیف لیکرت، عدد ۳ نمایانگر حد متوسط است.

دوره‌های آموزشی، برگزار نکردن دوره‌های آموزشی یا تعداد اندک آنها، هزینه‌های زیاد پیاده‌سازی، نبود بودجهٔ مناسب در سازمان، برخوردار نبودن از کمیتهٔ راهبری شایسته، بی‌ثباتی مدیریت ارشد سازمان، ناهمخوانی ساختار سازمانی با نیازهای ISMS، نبود بلوغ سازمانی، کار زیاد و تداخل مسئولیت‌های کارکنان، ترس کارکنان از سخت‌شدن فرایندهای کار، همکاری‌نداشتن و ناهماهنگی کارکنان درگیر پروژه، مقاومت مدیران و کارکنان در برابر تغییر، پایین‌بودن میزان رضایت شغلی کارکنان، تقلیل مفهوم ISMS به پروژهٔ امنیت شبکه و بی‌تمایلی سازمان به بازمهندسی فرایندهایش، موانع پیاده‌سازی ISMS معرفی شدند.

با توجه به کمبود پژوهش تجربی و اهمیت امنیت اطلاعات برای سازمان‌های امروزی، به‌ویژه شرکت ملی نفت ایران، این مطالعه در جست‌وجوی موانع استقرار سیستم مدیریت امنیت اطلاعات، اولویت‌بندی آن و بررسی میزان آمادگی مدیریت اکتشاف شرکت ملی نفت ایران در پیاده‌سازی این سیستم است؛ نتایج این پژوهش می‌تواند یاری‌دهندهٔ سازمان‌های دیگر برای سنجش میزان آمادگی پیاده‌سازی این سیستم باشد.

پیشینهٔ پژوهش

پیشینهٔ نظری

برای محافظت از اطلاعات سازمان، نمی‌توان به نوع خاصی از امنیت یا به یک محصول خاص اکتفا کرد (میوالد، ۱۳۸۳). بحث مدیریت امنیت اطلاعات به‌دلیل پیچیدگی زیاد، با مسائل بحث‌انگیز زیادی مواجه می‌شود که این مباحث درراستای فراهم‌آوردن چارچوب، روش و فناوری‌هایی برای بهبود پیاده‌سازی امنیت اطلاعات در سازمان است (چاو، ۲۰۰۵). پیاده‌سازی اثربخش امنیت اطلاعات، به رویکردی یکپارچه نیاز دارد (ورمولن و ونسلمز، ۲۰۰۲). در وضعیت کنونی، امنیت اطلاعات ماهیتی مدیریتی پیداکرده و به آموزش و توجه مدیران سازمان‌ها نیازمند است (کنپ، مارشال، رینر، مورا، ۲۰۰۴).

نبود حمایت مستمر مدیریت ارشد، یکی از موانعی است که کوک و لانگلی در سال ۱۹۹۹ و بلون در سال ۲۰۰۸ به‌طور مشترک بر آن تأکید کرده‌اند. همچنین به باور سیپونن و ویلسون (۲۰۰۹) چنانچه دانش و آگاهی کافی دربارهٔ سیستم مدیریت امنیت اطلاعات وجود نداشته باشد، سازمان هنگام پیاده‌سازی این استاندارد با مشکلاتی مواجه خواهد شد. عاملی که به عقیدهٔ بلون نیز از اهمیت بسیار بالایی برخوردار است (بلون، ۲۰۰۸؛ سیپونن و ویلسون، ۲۰۰۹ و کوک و لانگلی، ۱۹۹۹). ترس از بروز تغییرات در فرایندهای کسب‌وکار مانع دیگری است که ویلیام در سال ۲۰۰۸ به آن اشاره کرده است (ویلیام، ۲۰۰۸).

پیشینهٔ تجربی

با توجه به بررسی مبانی نظری و پیشینهٔ پژوهش، در ادامه به مستندات مربوط به موانع پیاده‌سازی سیستم مدیریت امنیت پرداخته می‌شود.

پژوهش‌های پیشین، موارد زیر را موانع پیاده‌سازی ISMS معرفی کرده‌اند:

تعیین اشتباه حوزهٔ انجام پروژه، نگرش نامناسب سازمان به این سیستم، آگاهی‌نداشتن و آموزش کم کارمندان سازمان، مقاومت کارمندان سازمان، تجهیزات نامناسب فنی، مدیریت ریسک نامناسب، عدم انجام ممیزی دوره‌ای، مقاومت کارمندان سازمان، بروز تغییرات در تشکیلات سازمانی، نداشتن درک صحیح از شروط و مفاد استاندارد، سازگار نبودن با رویه های سازمانی، هزینه‌های بالای مالی و زمانی پیاده‌سازی، برون‌سپاری خدمات IT، برخوردار نبودن از دانش کافی دربارهٔ تهدیدهای امنیت اطلاعات، فهرست دارایی ناقص، انتخاب کنترل‌های نامناسب، نبود برنامهٔ مناسب مدیریت تداوم کسب‌وکار، مستندسازی نامناسب، شرح وظایف و مسئولیت های نامناسب امنیتی، ممیزی های ناکافی مدیریت، مدیریت پروژهٔ نامناسب، پشتیبانی نامناسب مدیریت، ممیزی نامناسب داخلی، نظرخواهی‌نکردن از کارکنان دیگر سازمان هنگام اخذ تصمیمات مرتبط با امنیت اطلاعات، هم‌راستا نبودن سیاست‌های امنیتی با فلسفهٔ سازمانی، پراکندگی جغرافیایی سازمانی، نظارت ناکافی بر رفتار کارکنان در حوزهٔ امنیت اطلاعات و تخصیص نادرست مسئولیت‌های کاربران در حوزهٔ امنیت اطلاعات (الاین، ۲۰۰۹؛ دهیلن، ۲۰۰۱؛ عبدالجلیل و عبدالحمید، ۲۰۰۵؛ فومین، دیوریسو بارلت، ۲۰۰۸؛ کاکار، پونهانی و مدن، ۲۰۱۲؛ کریتزینگر، ۲۰۰۸؛ کو، چانگ و ین ، ۲۰۰۹).

همچنین موارد زیر عوامل حیاتی موفقیت پیاده‌سازی ISMS، شناسایی شدند: پشتیبانی و مشارکت مدیریت عالی سازمان، سیاست های مناسب امنیتی، شرح وظایف مناسب امنیتی، انگیزهٔ کارمندان، سازگاری رویهٔ کسب‌وکار سازمان با رویه‌های امنیتی و مشاور مجرب خارجی (العودی و ریناد، ۲۰۰۷؛ کاظمی، خواجویی و نصرآبادی، ۲۰۱۲).

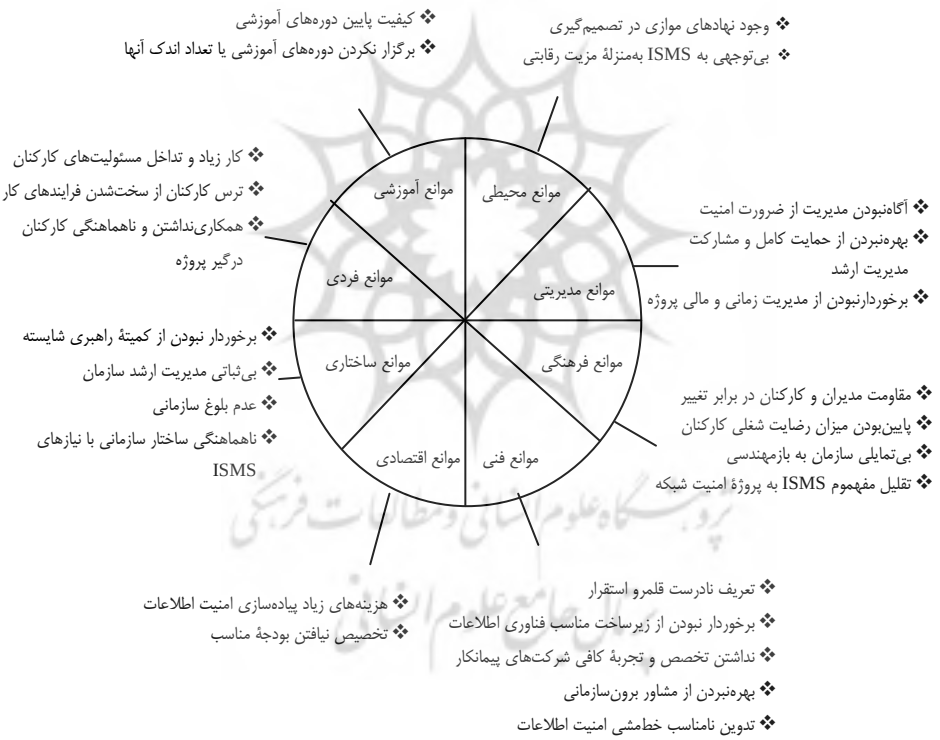
و موارد زیر نیز عوامل مؤثر بر پیاده‌سازی ISMS معرفی شدند:

نگهداری سیستم امنیت اطلاعات، سازگاری با قوانین دولتی، مدیریت تداوم کسب وکار، کنترل دسترسی، امنیت فیزیکی و محیطی، امنیت ارتباطات، مدیریت دارایی، امنیت منابع انسانی، ساختار امنیتی سازمان، سیاست‌های امنیتی و آموزش، فرهنگ سازمانی و ملی، تعهد مدیریت، مهارت و آموزش، آگاهی از مسئولیت‌ها، تشکیلات امنیت اطلاعات، تسهیم اطلاعات دانش، فناوری امنیت اطلاعات و مدیریت تغییرات، ساختار سازمانی، سیاست برخورد با ریسک، انجام کار تیمی، ناظر فنی سازمان، مدیریت سازمان، مشاور فنی سازمان، پیمانکار، حمایت مدیریت عالی،

آموزش امنیتی، فرهنگ امنیتی، مهارت امنیتی، تقویت خط‌مشی امنیتی، تجربه‌ها و خودباوری افراد، افزایش میزان آگاهی مدیریت و دانش کاربران (آلفاواز، ۲۰۱۱؛ چویی، کیم و گو، ۲۰۰۸؛ صدر عاملی، ترک لادانی و فراهی، ۱۳۸۸؛ طاهری، ۱۳۸۸؛ محسنی، ۲۰۱۳).

مدل مفهومی

مدل استاندارد و یکپارچه‌ای در زمینهٔ موانع پیاده‌سازی ISMS وجود ندارد و هریک از محققان پیشین تنها به بررسی بخشی از ابعاد مدل پرداخته‌اند. با توجه به بررسی مبانی نظری و پیشینهٔ پژوهش، مدل مفهومی در قالب شکل ۱ به نمایش گذاشته شده است.



شکل ۱. مدل مفهومی پژوهش

روش‌شناسی پژوهش

در این پژوهش برای جمع‌آوری داده‌های مربوط به مبانی نظری و استخراج عوامل و شاخص‌های اولیه، از منابع کتابخانه‌ای و اینترنتی شامل کتب، مقالات و مطالعات موردی بهره‌جویی شده است. به‌کمک ماتریس مقایسات زوجی به روش تحلیل سلسله‌مراتبی، به اولویت‌بندی موانع پیاده‌سازی ISMS پرداخته شد و برای بررسی میزان آمادگی مدیریت اکتشاف شرکت ملی نفت ایران در پیاده‌سازی ISMS، از ابزار پرسشنامه استفاده شده است.

ابتدا طرح اولیهٔ پرسشنامهٔ میزان آمادگی پیاده‌سازی ISMS تهیه شد و پس از بررسی کارشناسانهٔ استادان راهنما و مشاور و نیز، سایر خبرگان و اعمال اصلاحات لازم در بخش‌های گوناگون، پرسشنامهٔ نهایی تدوین شد. برای محاسبهٔ پایایی پرسشنامه از روش آلفای کرونباخ استفاده شده است. مقدار آلفا برای پرسشنامهٔ پژوهش برابر با ۰/۸۶۶ به‌دست آمد که رقم پایایی بالای پرسشنامه را نشان می‌دهد.

تجزیه و تحلیل اطلاعات، آزمون فرضیه‌های پژوهش و توصیف آنها به روش‌های آماری گوناگونی انجام گرفت که عبارتند از:

- بررسی روایی ابزار اندازه‌گیری با روایی ظاهری[1]؛
- بررسی پایایی ابزار اندازه‌گیری با محاسبهٔ ضریب آلفای کرونباخ[2]؛
- ارائهٔ آماره‌های توصیفی، شامل میانگین، انحراف معیار، مقایسهٔ میانگین یک متغیر با استفاده از آزمون تی. تک‌نمونه‌ای[3]؛
- مقایسهٔ میانگین متغیر بیش از دو گروه وابسته با استفاده از آزمون اندازه‌های تکراری[4]؛
- اولویت‌بندی عوامل با استفاده از روش تحلیل سلسله‌مراتبی (AHP)[5].

یافته‌های پژوهش

به‌منظور اولویت‌بندی موانع پیاده‌سازی ISMS، پس از تعیین معیارهای اصلی و زیر معیارها و دریافت نظرات هریک از خبرگان در قالب جدول مقایسات زوجی، به تجزیه و تحلیل اطلاعات به‌دست‌آمده اقدام شد. در جمع‌آوری جداول، وزن متفاوتی برای افراد در نظر گرفته نشد و همه با یکدیگر ادغام شدند. در جدول ۱ و جدول ۲ نتایج اولویت‌بندی موانع آمده است.

---

1. Face validity
2. Cronbach's Alpha
3. One-sample t test
4. Repeated Measures
5. Analytical Hierarchy Process

جدول ۱. رتبه‌بندی موانع اصلی و زیر عامل‌ها

وزن عوامل اصلی	عوامل اصلی	زیر عامل	وزن زیر عامل‌ها
۰/۲۴۷	موانع ساختاری	ناهماهنگی ساختار سازمانی با نیازهای سیستم مدیریت امنیت اطلاعات	۰/۴۸۷
		عدم بلوغ سازمانی	۰/۱۸۳
		برخوردار نبودن از کمیتهٔ راهبری شایسته	۰/۱۷۵
		بی‌ثباتی مدیریت ارشد سازمان	۰/۱۵۵
۰/۱۶۶	موانع فرهنگی	مقاومت مدیران و کارکنان در برابر تغییر	۰/۴۴۴
		پایین‌بودن میزان رضایت شغلی کارکنان	۰/۲۰۸
		تقلیل مفهوم سیستم مدیریت امنیت اطلاعات به پروژهٔ امنیت شبکه	۰/۱۹۸
		بی‌تمایل بودن سازمان به باز مهندسی فرایندهایش	۰/۱۵۰
۰/۱۴۱	موانع فنی	نداشتن تخصص و تجربهٔ کافی شرکت‌های پیمانکار	۰/۲۵۹
		برخوردار نبودن از زیرساخت مناسب فناوری اطلاعات	۰/۲۵۰
		تدوین نامناسب خط‌مشی امنیت اطلاعات	۰/۲۲۲
		بهره‌نبردن از مشاور برون‌سازمانی	۰/۱۶۵
		تعریف نادرست قلمرو استقرار سیستم مدیریت امنیت اطلاعات	۰/۱۰۴
۰/۱۱۰	موانع فردی	کار زیاد و تداخل مسئولیت‌های کارکنان	۰/۶۰۵
		همکاری‌نداشتن و ناهماهنگی کارکنان درگیر پروژه	۰/۲۲۱
		ترس کارکنان از سخت‌شدن فرایندهای کار	۰/۱۷۴
۰/۰۹۶	موانع آموزشی	برگزار نکردن دوره‌های آموزشی یا تعداد اندک آنها	۰/۵۵۰
		کیفیت پایین دوره‌های آموزشی	۰/۴۵۰
۰/۰۹۳	موانع اقتصادی	تخصیص‌نیافتن بودجهٔ مناسب در سازمان	۰/۶۷۰
		هزینه‌های زیاد پیاده‌سازی	۰/۳۳۰
۰/۰۷۹	موانع محیطی	بی‌توجهی به سیستم مدیریت امنیت اطلاعات به‌منزلهٔ مزیت رقابتی	۰/۵۳۶
		وجود نهادهای موازی در تصمیم‌گیری (فناوری اطلاعات و حراست)	۰/۴۶۴
۰/۰۶۸	موانع مدیریتی	برخوردار نبودن از مدیریت زمانی و مالی پروژه	۰/۳۹۱
		بی‌بهره‌بودن از حمایت کامل و مشارکت مدیریت ارشد	۰/۳۰۷
		ناآگاهی مدیریت به ضرورت امنیت	۰/۳۰۲

جدول ۲. رتبه‌بندی نهایی زیر عامل‌ها

نام عامل	وزن نهایی	اولویت
ناهماهنگی ساختار سازمانی با نیازهای سیستم مدیریت امنیت اطلاعات	۰/۱۱۰	۱
مقاومت مدیران و کارکنان در برابر تغییر	۰/۰۷۴	۲
نداشتن تخصص و تجربهٔ کافی شرکت‌های پیمانکار	۰/۰۶۳	۳
برخوردار نبودن از زیرساخت مناسب فناوری اطلاعات	۰/۰۶۰	۴
تدوین نامناسب خط‌مشی امنیت اطلاعات	۰/۰۵۴	۵
کار زیاد و تداخل مسئولیت‌های کارکنان	۰/۰۴۹	۶
برگزار نکردن دوره‌های آموزشی یا تعداد اندک آنها	۰/۰۴۳	۷
تخصیص نیافتن بودجهٔ مناسب در سازمان	۰/۰۴۲	۸
عدم بلوغ سازمانی	۰/۰۴۱	۹
بهره‌نبردن از مشاور برون‌سازمانی	۰/۰۴۰	۱
برخوردار نبودن از کمیتهٔ راهبری شایسته	۰/۰۴۰	۱۱
بی‌توجهی به سیستم مدیریت امنیت اطلاعات به‌منزلهٔ مزیت رقابتی	۰/۰۳۶	۱۲
کیفیت پایین دوره‌های آموزشی	۰/۰۳۵	۱۳
بی‌ثباتی مدیریت ارشد سازمان	۰/۰۳۵	۱۴
پایین‌بودن میزان رضایت شغلی کارکنان	۰/۰۳۵	۱۵
تقلیل مفهوم سیستم مدیریت امنیت اطلاعات به پروژهٔ امنیت شبکه	۰/۰۳۳	۱۶
وجود نهادهای موازی در تصمیم‌گیری (فناوری اطلاعات و حراست)	۰/۰۳۱	۱۷
برخوردار نبودن از مدیریت زمانی و مالی پروژه	۰/۰۳۰	۱۸
تعریف نادرست قلمرو استقرار سیستم مدیریت امنیت اطلاعات	۰/۰۲۵	۱۹
بی‌تمایل بودن سازمان به بازمهندسی فرایندهایش	۰/۰۲۵	۲۰
برخوردار نبودن از حمایت کامل و مشارکت مدیریت ارشد	۰/۰۲۴	۲۱
ناآگاهی مدیریت به ضرورت امنیت	۰/۰۲۳	۲۲
هزینه‌های زیاد پیاده‌سازی	۰/۰۲۰	۲۳
همکاری‌نکردن و ناهماهنگی کارکنان درگیر پروژه	۰/۰۱۸	۲۴
ترس کارکنان از سخت‌شدن فرایندهای کار	۰/۰۱۴	۲۵

در جدول ۳ نتایج آزمون فرضیهٔ سوم (سطح همهٔ مؤلفه‌های آمادگی مدیریت اکتشاف شرکت ملی نفت ایران در پیاده‌سازی سیستم مدیریت امنیت اطلاعات بیشتر از حد متوسط است)، درج شده است. این نتایج به‌کمک آزمون تی. تک‌نمونه‌ای به‌دست آمده است.

جدول۳. آزمون فرض آمادگی کل و مؤلفه‌های آن

	میانگین	آمارهٔ آزمون	درجه آزادی	مقدار احتمال
آمادگی کل	۳/۱۳۲	۱/۴۲۰	۲۶	۰/۰۸۴
اقتصادی	۳/۴۴۴	۲/۶۵۵	۲۶	۰/۰۰۷
فنی	۳/۴۱۵	۳/۸۸۷	۲۶	<۰/۰۰۱
محیطی	۳/۲۷۸	۲/۳۰۸	۲۶	۰/۰۱۵
فردی	۳/۱۸۵	۱/۱۶۹	۲۶	۰/۱۲۷
ساختاری	۳/۱۵۸	۱/۶۴۹	۲۶	۰/۰۵۶
مدیریتی	۳/۰۱۲	۰/۰۸۹	۲۶	۰/۴۶۵
فرهنگی	۲/۸۶۱	-۱/۱۲۷	۲۶	۰/۸۶۵
آموزشی	۲/۵۵۶	-۲/۶۹۰	۲۶	۰/۹۹۴

با توجه به جدول ۳، میزان آمادگی سازمان در مؤلفه‌های مدیریتی، آموزشی، ساختاری، فردی و فرهنگی کمتر از حد متوسط است، بنابراین فرضیهٔ سوم، در سطح معناداری ۰/۰۵ برای این مؤلفه‌ها تأیید نمی‌شود. همچنین میزان آمادگی سازمان در مؤلفه‌های محیطی، فنی و اقتصادی بیشتر از حد متوسط است، بنابراین فرضیهٔ سوم برای این مؤلفه‌ها در سطح معناداری ۰/۰۵ تأیید می‌شود.

برای اینکه مشخص شود، میانگین ۸ مؤلفهٔ آمادگی پیاده‌سازی سیستم مدیریت امنیت اطلاعات باهم برابرند، ابتدا آزمون کرویت[1] انجام می‌گیرد و پس از آن، به آزمون فرض تساوی میانگین ۸ مؤلفهٔ مذکور پرداخته می‌شود، چنانچه تساوی ۸ میانگین رد شود، با استفاده از آزمون تعقیبی[2] به مقایسهٔ دوبه‌دوی میانگین‌ها پرداخته می‌شود (جدول ۴).

جدول٤. آزمون ماوچلی[3] برای بررسی کرویت

آمارهٔ ماوچلی	آمارهٔ تقریبی خی‌دو	درجه آزادی	مقدار احتمال
۰/۰۸۱	۵۸/۸۶۴	۲۷	<۰/۰۰۱

با توجه به مقدار احتمال در جدول ۴، فرض کرویت رد می‌شود، بنابراین برای مقایسه میانگین‌ها از آزمون گرینهاوس ـ گیزر[4] استفاده می‌شود.

---

1. Sphericity
2. Post hoc
3. Mauchly's test
4. Greenhouse-Geisser

جدول ٥. آزمون گرینهاوس ـ گیزر برای مقایسهٔ میانگین ٨ مؤلفهٔ مذکور

مجموع مربعات	درجه آزادی	میانگین مربعات	آمارهٔ آزمون	مقدار احتمال
۱۶/۷۲۹	۳/۸۹۰	۴/۳۰۰	۸/۰۵۷	<۰/۰۰۱

با توجه به مقدار احتمال جدول ٥، فرض برابری میانگین ٨ مؤلفه مذکور رد می‌شود، به بیان دیگر، حداقل میانگین دو تا از مؤلفه ها باهم برابر نیستند. حال به مقایسهٔ دوبه‌دوی میانگین مؤلفه‌ها پرداخته می‌شود.

جدول ٦. مقایسهٔ دوبه‌دوی میانگین مؤلفه‌های مذکور

مؤلفهٔ اول	مؤلفهٔ دوم	مقدار احتمال (p-value)
مدیریتی	محیطی	۰/۰۳۶
	فنی	۰/۰۰۱
	آموزشی	۰/۰۰۶
	اقتصادی	۰/۰۰۷
	ساختاری	۰/۲۵۲
	فردی	۰/۳۰۰
	فرهنگی	۰/۳۵۶
محیطی	فنی	۰/۲۲۱
	آموزشی	۰/۰۰۱
	اقتصادی	۰/۳۷۱
	ساختاری	۰/۳۶۹
	فردی	۰/۴۸۳
	فرهنگی	۰/۰۱۴
فنی	آموزشی	<۰/۰۰۱
	اقتصادی	۰/۸۳۴
	ساختاری	۰/۰۰۴
	فردی	۰/۰۶۳
	فرهنگی	<۰/۰۰۱
آموزشی	اقتصادی	<۰/۰۰۱
	ساختاری	۰/۰۰۱
	فردی	۰/۰۰۷
	فرهنگی	۰/۰۳۳
اقتصادی	ساختاری	۰/۰۷۷
	فردی	۰/۲۰۹
	فرهنگی	۰/۰۰۲
ساختاری	فردی	۰/۸۳۸
	فرهنگی	۰/۰۲۰
فردی	فرهنگی	۰/۰۴۱

در مقایسهٔ میانگین‌های مؤلفه‌های مشخص‌شده در جدول ۶، هر نتیجه‌ای که مقدار احتمال آن کمتر از ۰/۰۵ بود، فرض برابری میانگین آن دو مؤلفه در سطح معنی‌داری ۰/۰۵ رد می‌شود.

نتیجه‌گیری و پیشنهادها

به طور خلاصه نتایج پژوهش حاضر به شرح زیر است:

۱. از میان موانع ساختاری، فرهنگی، فنی، فردی، آموزشی، اقتصادی، محیطی و مدیریتی، موانع ساختاری شامل مؤلفه‌های ناهمخوانی ساختار سازمانی با نیازهای ISMS، عدم بلوغ سازمانی، برخوردار نبودن از کمیتهٔ راهبری شایسته و بی‌ثباتی مدیریت ارشد سازمان با مقدار ۰/۲۴۷، مهم‌ترین مانع اصلی پیاده‌سازی ISMS شناخته شد و مانع مدیریتی شامل مؤلفه‌های برخوردارنبودن از مدیریت زمانی و مالی پروژه، بهره‌نبردن از حمایت کامل و مشارکت مدیریت ارشد و ناآگاهی مدیریت به ضرورت امنیت با مقدار ۰/۰۶۸، پایین‌ترین رتبه در بین موانع پیاده‌سازی ISMS را داشته است.

۲. از میان ۲۵ مؤلفهٔ موانع پیاده‌سازی ISMS، ناهمخوانی ساختار سازمانی با نیازهای ISMS (۰/۱۱۰)، مهم‌ترین مانع پیاده‌سازی ISMS بوده است و ترس کارکنان از سخت‌شدن فرایندهای کار با اجرای ISMS (۰/۰۱۴)، پایین‌ترین رتبه را داشته است.

۳. مدیریت اکتشاف شرکت ملی نفت ایران در زمینهٔ پیاده سازی ISMS آمادگی لازم را ندارد.

۴. مدیریت اکتشاف شرکت ملی نفت ایران در زمینهٔ پیاده‌سازی ISMS از لحاظ مدیریتی، آموزشی، ساختاری، فردی و فرهنگی آمادگی کمتر از حد متوسط را دارد؛ بنابراین باید به‌ترتیب در زمینه‌های آموزشی، فرهنگی، مدیریتی، ساختاری و فردی، تمرکز و توجه بیشتری شود.

۵. مدیریت اکتشاف شرکت ملی نفت ایران در زمینهٔ پیاده سازی ISMS از لحاظ محیطی، فنی و اقتصادی، آمادگی بیشتر از حد متوسطی دارد.

۶. بین مؤلفه‌های مدیریتی ـ ساختاری، مدیریتی ـ فردی، مدیریتی ـ فرهنگی، محیطی ـ فنی، محیطی ـ اقتصادی، محیطی ـ ساختاری، محیطی ـ فردی، فنی ـ اقتصادی، فنی ـ فردی، اقتصادی ـ ساختاری، اقتصادی ـ فردی و ساختاری ـ فردی، تفاوت معنادار آماری وجود ندارد.

با توجه به نتایج به‌دست‌آمده از پژوهش، برای اجرای ISMS در مدیریت اکتشاف شرکت ملی نفت ایران موارد زیر پیشنهاد می‌شود:

۱. سازمان در جذب نیروهای متخصص فناوری اطلاعات، دقت لازم را داشته باشد و در سطح تشکیلات امنیت فناوری اطلاعات در سه سطح سیاستگذاری (کمیتهٔ راهبردی)، مدیریت

اجرایی (مدیر امنیت) و فنی (واحد پشتیبانی امنیت) بازنگری کند، همچنین تشکیلات لازم برای ایجاد و تداوم امنیت فضای تبادل اطلاعات سازمان را فراهم آورد.

۲. سازمان در راستای افزایش بلوغ سازمانی با انجام تمهیدات لازمی چون، برگزاری دوره‌های آموزشی و سمینارهای تخصصی ISMS برای مدیران و کارکنان در سطوح مختلف در حد کفایت و کیفیت مناسب، اقدامات مؤثری انجام دهد.

۳. مدیران سازمانی از فضای تبادل اطلاعات احساس ناامنی نمی‌کنند و مایملک اطلاعاتی گرانبهای سازمان را در معرض تهاجم نمی‌بینند. بر این اساس، در زمینهٔ پیاده‌سازی و تداوم استانداردهای مدیریت امنیت حمایت جدی و همه‌جانبه‌ای نمی‌کنند. بنابراین مدیران شرکت باید در مورد ارزشی که از سیستم ISMS در مقابل مأموریت سازمان و اهداف عملیاتی می‌خواهند، مواضع روشنی داشته باشند؛ ضمن آنکه فواید پیاده‌سازی ISMS برای مدیران و کارکنان تشریح شود تا چشم‌اندازی روشن و خوب از سازمان پس از پیاده‌سازی ISMS ارائه شود.

۴. امنیت پیش از آنکه نوعی فناوری باشد، فرهنگ است. بنابراین باید با همهٔ رؤسا و معاونت‌ها برای آشنایی و بهبود عملکرد مؤثر این سیستم مدیریتی، ارتباط برقرار شود.

۵. ارائهٔ گزارش‌های نظام‌مند، تحلیلی و مستمر به مدیریت ارشد سازمان و جلب حمایت و مشارکت او لازم است.

۶. باید کمیتهٔ راهبری و ممیزی تشکیل شود و برای افزایش انگیزه و رضایت شغلی افراد این کمیته‌ها اقدامات لازم صورت گیرد.

۷. روحیهٔ همکاری، مشارکت و کارگروهی در بین افراد سازمان باید تشویق و تقویت شود.

۸. مراحل امن‌سازی؛ نحوهٔ شکل‌گیری چرخهٔ امنیت اطلاعات و ارتباطات سازمان؛ جزئیات مراحل امن‌سازی؛ روش‌های فنی به‌کار رفته در هر مرحله؛ فهرست و محتوای طرح‌ها و برنامه‌های امنیتی سازمان، جزئیات ایجاد تشکیلات سیاستگذاری، اجرایی و فنی امنیت اطلاعات و ارتباطات سازمان و کنترل‌های امنیتی برای هر یک از سیستم‌های اطلاعاتی و ارتباطی سازمان به‌صورت دقیق مشخص شود.

۹. مستند محدودهٔ فیزیکی و سازمانی ISMS، مستند آموزش‌های سازمان در زمینهٔ امنیت و مستند دقیق و کافی تشکیلات سازمانی مدیریت امنیت اطلاعات، مشخص شود.

۱۰. امنیت نامحسوس است، بنابراین وقتی یک پروژهٔ امنیتی (از نوع مدیریت امنیت) اجرا می‌شود، بعضی مواقع مدیریت سازمان و کارشناسان احساس می‌کنند که هیچ اتفاق جدیدی رخ نداده است و از اینکه برای اجرای آن هزینه کرده‌اند، احساس ندامت می‌کنند. برای پاسخ به این

دسته از افراد باید فکر کرد اگر روی مسئلهٔ امنیت کار نمی‌شد، چه اتفاقی ممکن بود بیفتـد. پـس باید در هر زمان و در هر مکان از فضای تبادل اطلاعات سازمانی به فکر امنیت بود.

References

Abduljalil, S. & Abdulhamid, R. (2005 & 2007). *ISMS Pilot Program Experiences: Benefits, Challenges & Recommendations.* 2013, from http://cybersecurity.my/data/content_files/11/23.pdf.

Al-Awadi, M. & Renaud, K. (2007). *Success factors in information security implementation in organizations*. Paper presented at the IADIS International Conference e-Society 2007, Available in: http://www.dcs.gla.ac.uk /~karen/ Papers/sucessFactors2.pdf.

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.

Bellone, J. (2008). A practiced approach to information security management system implementation. *Information Management & Computer Security*, 16 (1): 49-57.

Chau, J. (2005). Skimming the technical and legal aspects of BS7799 can give a false sense of security. *Computer Fraud & Security*, 9: 8-10.

Choi, N., Kim, D. & Goo, J. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*, 16 (5): 484-485.

Dhillon, G. (2001). Information security management: global challenges in the new millennium, *IGI Global*, DOI: 10.4018/978-1-878289-78-0.

Ernest-Jones, T. (2006). Pinning down a security policy for mobile data, *Network Security*, 2006 (6): 8-13.

Fomin, V., DeVries, H., Barlette, Y. (2008). *ISO/IEC 27001 Information systems security management standards: Exploring the reasons for low adoption*. RSM Erasmus University, Netherland.

Honan, B. (2006). *IT security-commoditized, badly Infosecurity Today*, 3 (5): 41.

ISO/IEC 27001: 2013: *Information technology — Security techniques — Information security management systems—Requirements*, http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534.

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.

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.

Khorasani Rad, A., Hossein Abadi, H. & Amirzadeh, R. (1996). *Standard ISO / IEC 27001:2005*. Partner company Tuff Iran (Member of TUV Nord), Tehran. (*in Persian*)

Knapp, K. J., Marshall, T. E., Rainer, R. K. & Morrow, D. W. (2004). *Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC) Survey Results*. Auburn University, Auburn, AL.

Kotonya, G. & Sommerville, I. (1998). *Requirements Engineering Process and Techniques*. Hardcover, ISBN: 978-0-471-97208-2, http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0471972088.html#instructor.

Kraemer, S.B. (2006). *An adversarial viewpoint of human and organizational factors in computer and information security*. A dissertation for the degree of Doctor Philosophy at the university of Wisconsin-Madison.

Kritzinger, E. & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, 27 (5): 224-231.

Ku, C., chang, Y., Yen, D. (2009). National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy*, 33 (7): 371-384.

Kwok, L. & Longley, D. (1999). Information security management and modeling. *Information Management & Computer Security*, 7 (1): 30-40.

Mivald, A. (2004). *Computer network security*, Translated by Seyyed Ahmad Safai, The first edition, Daneshparvar, Tehran. (*in Persian*)

Mohseni, M. (2013). *Has your organization compliance with ISMS? A case study in an Iranian Bank*. arXiv preprint arXiv:1303.0468. from Http://arxiv.org/ftp/arxiv/papers/1303/1303.0468.pdf.

Ryan, J. (2006). *A comparison of information security trends between formal and informal environments*. A Dissertation for the Degree of Doctor of Philosophy the Graduate, Faculty of Auburn University Alabama.

Sadr-Ameli, F., Tork Ladany, B. & Farahi, A. (2009). *Challenges and succes factors for implementation of Information Security Management System (ISMS) in Iran a by hierarchical analysis method (AHP).* Sixth International Conference on Management of Information and Communication Technology, Tehran, Institute of Management Technology, http://www.civilica.com/ Paper-ICTM06-ICTM06_142.html. (*in Persian*)

Siponen, M. & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46 (5): 267-270.

Taheri, M. (2009). *Provide a framework for the role of human factors in information systems security*. MA thesis, Tarbiat Modarres University, Faculty of Humanities. (*in Persian*)

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.

Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computer and Security*, 26 (3): 256-265.