ارزیابی سیستم‌های مدیریت اطلاعات دانشگاه علوم پزشکی اصفهان با استفاده از استاندارد ISO/IEC 27001*

روح‌اله شیخ ابومسعودی[1]، سحر کوهی‌حبیبی[2]، مریم عطایی[2]، نازیلا اسماعیلی[2]

مقاله پژوهشی

چکیده

مقدمه: با توجه به خطرات تهدیدکننده اطلاعات و نیاز مبرم به رویه‌های ایجاد و تقویت امنیت و محرمانگی، سازمان بین المللی استاندارد (ISO: International Organization for Standardization) اقدام به تدوین استانداردی در زمینه امنیت اطلاعات تحت عنوان ISO/IEC 27001 نموده است. کسب تأییده ممیزی این استاندارد دارای منافع بسیار زیادی برای سازمان بوده و علاوه بر شناسایی عیوب موجود در بخش‌ها و فرآیندهای اطلاعاتی، باعث افزایش اعتبار سازمان در محیط رقابتی و ایجاد مزیت رقابتی می گردد. هدف از این پژوهش ارزیابی سیستم‌های مدیریت اطلاعات دانشگاه علوم پزشکی اصفهان با استفاده از استاندارد ISO/IEC 27001 در سال ۱۳۹۰ خورشیدی بوده است.

روش بررسی: این پژوهش کاربردی و از دسته مطالعات توصیفی-کیفی است. جامعه پژوهش کلیه بخش‌های فناوری اطلاعات دانشگاه علوم پزشکی اصفهان، شامل مراکز کامپیوتر دانشکده‌ها (۹ مرکز)، بیمارستان‌ها (۱۳ مرکز) و مرکز آمار و اطلاع رسانی (جمعا ۲۳ مرکز) در سال ۱۳۹۰ خورشیدی، می‌باشد. ابزار گردآوری اطلاعات در این پژوهش استاندارد ISO/IEC 27001: 2005 می‌باشد که در قالب چک لیست بین المللی ارائه شده است. چک لیست مورد استفاده دارای ۱۱ بخش اصلی است که هر کدام در برگیرنده چندین بخش فرعی و سؤال می‌باشد. داده‌ها از طریق مصاحبه و همچنین مشاهده و مستندات پژوهشگران، گردآوری و به کمک نرم‌افزار Excel ۲۰۱۰ تجزیه و تحلیل گردید.

یافته‌ها: نتایج ممیزی مرکز آمار و اطلاع رسانی دانشگاه علوم پزشکی اصفهان نشان می‌دهد که این سازمان در حیطه‌های اصلی استاندارد که عبارتند از سیاست امنیتی، تشکیلات امنیت اطلاعات، مدیریت سرمایه، امنیت منابع انسانی، امنیت محیطی و فیزیکی، مدیریت عملیات‌ها و ارتباطات، کنترل دسترسی، بکارگیری، توسعه و نگهداری از سیستم‌های اطلاعاتی، مدیریت رویداد امنیت اطلاعات، مدیریت استمرار کسب و کار و تطابق توانسته است به ترتیب ۳۱، ۴۰، ۲۸، ۶۵، ۷۳، ۵۴، ۵۴، ۴۴، ۵۸، ۳۸ و ۵۴ درصد از موارد مورد نظر را اجرایی نماید.

نتیجه‌گیری: با توجه به اهمیت استاندارد جهانی ISO/IEC 27001 در استقرار فرآیندهای مبتنی بر امنیت اطلاعات و حفظ محرمانگی، یکپارچگی و دسترس‌پذیری، سازمان می‌بایستی تلاش بیشتری را نسبت به بکارگیری آن در فرآیندهای خود معطوف دارد. نتایج نشان دهنده ی این موضوع هستند که جز در حیطه های امنیت منابع انسانی و همچنین امنیت محیطی و فیزیکی، سازمان عملکرد خوبی در قبال مدیریت امنیت اطلاعات در فرآیندهای داخلی خود نداشته است.

واژه‌های کلیدی: ارزیابی؛ سیستم مدیریت اطلاعات؛ استانداردها.

دریافت مقاله: ۹۲/۱۲/۲۹ اصلاح نهایی: ۹۳/۱۰/۲۵ پذیرش مقاله: ۹۳/۱۱/۱۳

ارجاع: شیخ ابومسعودی روح اله، کوهی حبیبی سحر، عطایی مریم، اسماعیلی نازیلا. **ارزیابی سیستم‌های مدیریت اطلاعات دانشگاه علوم پزشکی اصفهان با استفاده از استاندارد ISO/IEC 27001.** مدیریت اطلاعات سلامت ۱۳۹۴؛ ۱۲(۳): ۳۰۶-۳۱۶.

*- مقاله حاصل طرح تحقیقاتی شماره ی ۲۹۰۱۰۷ می باشد که توسط معاونت پژوهشی دانشگاه علوم پزشکی اصفهان حمایت شده است.

۱- مربی، صنایع، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران (نویسنده مسؤول) Email: abumasoudi@live.com

۲- کارشناس، فناوری اطلاعات سلامت، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

مقدمه

اطلاعات در سازمان‌ها، مؤوسسات پیشرفته و جوامع علمی شاهرگ حیاتی محسوب می‌گردد (۱). به طور کلی ارزش اطلاعات به منابع اطلاعات، مکان اطلاعات و زمان اطلاعات بستگی دارد (۲). در هر سازمان روزانه، اطلاعات زیادی تولید می‌شود و ضروری است نظام‌های اطلاعاتی قدرتمندی به وجود آید که بتواند این گونه اطلاعات را به طور صحیح و فوری پردازش کند و برای پیشبرد اهداف مدیریت سازمان، اطلاعات مفیدی فراهم سازد (۳). سازمان‌های آموزشی و دانشگاه‌ها نیز از این امر مستثنی نیستند و به اطلاعاتی صحیح، دقیق و روزآمد نیاز دارند تا بر مبنای آن بتوانند تصمیماتی بخردانه و درست بگیرند (۴).

در محیط کسب و کار الکترونیکی به هم پیوسته امروزی، نگرانی‌ها در خصوص امنیت در حال رشد است (۵). استفاده از فناوری اطلاعات ریسک‌های ویژه را برای سیستم‌های اطلاعات و به خصوص منابع حیاتی و مهم به همراه دارد که به دلیل ماهیت آن می‌باشد (۶). به همین دلیل امروزه بسیاری از سازمان‌ها به دنبال ایجاد سیستم‌های امنیتی برای جلوگیری از درز اطلاعاتشان به بیرون می‌باشند تا بتوانند کل مجموعه خود را حفظ کنند (۷). امنیت سیستم اطلاعات مانند یک زنجیره است که نقاط قوت آن تحت تأثیر نقاط ضعف قرار می‌گیرند (۸). دانشگاه علوم پزشکی اصفهان به عنوان یک سازمان دولتی، حجم وسیعی از اطلاعات را در سیستم‌های موجود در سازمان نگهداری می‌کند که به لحاظ اینکه با اطلاعات شخصی، تحصیلی و شغلی افراد مرتبط هستند، حفاظت بالایی را طلب می‌نماید. با توجه به قوانین مصوب مجلس شورای اسلامی و همچنین سازمان پدافند غیرعامل و از طرف دیگر حراست وزارتخانه بهداشت درمان و آموزش پزشکی، مرکز آمار و اطلاع رسانی دانشگاه‌های علوم پزشکی نهادی است که مسؤولیت تضمین امنیت اطلاعات را در کلیه حوزه‌های فیزیکی، نرم‌افزاری و سخت افزاری بر عهده دارد. از آنجا که اطلاعات موجود در این بخش دارای حساسیت بالایی می‌باشد، سنجش سطح امنیت آن و ارائه راهکارهای امنیتی جهت رفع نقایص و ضعف‌های موجود در این زمینه بسیار ضروری و همچنین ارزشمند به نظر می‌رسد. دستورالعمل‌های مدیریت امنیت اطلاعات بین‌المللی نقش مهمی در مدیریت و تأیید سیستم‌های اطلاعات سازمانی ایفا می‌کنند (۹). سیستم مدیریت امنیت اطلاعات (ISMS: Information Security Management System)، امنیت اطلاعات را به طور مداوم در زمینه فناوری، مدیریت، سخت‌افزار مدیریت می‌کند تا به هدف امنیت اطلاعات که دستیابی به محرمانگی، یکپارچگی و دسترس‌پذیری است دست یابد (۶). سازمان در کنار پیاده‌سازی و استفاده از سیستم مدیریت امنیت اطلاعات، باید در فواصل زمانی طرح‌ریزی شده سیستم را مورد بازنگری قرار دهد تا از تداوم تناسب، کفایت و اثربخشی آن اطمینان حاصل نماید (۱۰). ارزیابی یک جز ضروری در چرخه توسعه سیستم‌های اطلاعاتی و چرخه کیفیت می‌باشد و به دلایل گوناگون ارزیابی بازتاب پیشرفت فرآیندهای معین را ارائه می‌دهد (۱۱). استاندارد ISO/IEC 27001: 2005 یکی از چهارچوب‌های اساسی برای مدیریت امنیت اطلاعات در جهت کمک به سازمان‌ها در ارزیابی ریسک‌های امنیتی و پیاده‌سازی کنترل‌های امنیتی مناسب می‌باشد (۶). در ارزیابی فرآیند، توجه به درک این نکته معطوف می‌شود که فرآیند چگونه عمل می‌کند، چگونه تولید می‌کند و چه چیزی حاصل آن است؟ پس نیت در ارزیابی فرآیند سنجش پیشرفت، بهبود اثربخشی در جریان مداخله‌ها است و فقط پیامدهای درازمدت مورد نظر نیست (۱۲).

دیدگاه فرآیندگرایی که در این استاندارد بین‌المللی برای مدیریت امنیت اطلاعات ارائه شده، کاربران را ترغیب می‌کند که اهمیت مواردی از جمله درک الزامات امنیت اطلاعات سازمان و لزوم ایجاد خط‌مشی و اهداف برای امنیت اطلاعات، پیاده سازی و اجرای کنترل‌ها برای مدیریت مخاطرات کلان کسب و کار سازمان، پایش و بازنگری عملکرد و اثربخشی سیستم مدیریت امنیت اطلاعات و بهبود مستمر بر پایه اندازه‌گیری اهداف را مدنظر قرار دهند (۱۰).

شیخ‌پور و مدیری در مقاله‌ای تحت عنوان رویکردی جهت ترسیم نقشه‌ای بین فرآیندهای COBIT و کنترل‌های مدیریت امنیت اطلاعات ISO/IEC 27001 بیان می‌کنند که امنیت اطلاعات نقش مهمی در حفاظت از دارایی‌های سازمان دارد. از آنجایی که هیچ فرمولی وجود ندارد تا تأمین امنیت را به طور کامل تضمین نماید، نیاز به استفاده از محک‌ها و یا استانداردهایی برای کمک به اطمینان از تأمین سطح مناسبی از امنیت، استفاده مناسب از منابع و همچنین اتخاذ بهترین روش‌های امنیتی وجود دارد (۶). همچنین Kakkar و همکارانش در پژوهشی با عنوان پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کمبودهای عملی آن عنوان می‌کند که با استفاده از سیستم مدیریت امنیت اطلاعات، سازمان می‌تواند به تعیین سطوح امنیتی لازم پرداخته و دارایی‌هایش را با توجه به ممیزی صورت گرفته در خصوص ریسک‌های مربوطه توزیع نماید (۱۳). در پژوهشی دیگر Mellado و همکارانش در مطالعه‌ای با عنوان فرآیندی جهت مهندسی نیازمندی‌های امنیتی مبتنی بر معیار در راستای توسعه سیستم‌های اطلاعاتی ایمن را انجام دادند. آن‌ها بیان کردند که سازمان‌ها می‌بایستی یک فرآیند استاندارد جهت هماهنگی و برآورده ساختن نیازمندی‌های امنیت در مراحل نخستین فرآیند توسعه نرم‌افزار ایجاد نمایند. (۱۴). Von Solms، ده اشتباه مرگبار در مدیریت امنیت اطلاعات در مقاله‌ای با همین عنوان معرفی کرده است. او بیان می‌کند ایجاد و پیاده‌سازی یک برنامه امنیت اطلاعات مناسب الزاماً کار بسیار دشواری نمی‌باشد، اکثراً اجزای چنین برنامه‌ای بسیار بدیهی و معقول می‌باشند (۱۵).

Barnett و Adger در مطالعه‌ای تغییر آب و هوا، امنیت منابع انسانی و تعارضات و رفتارهای خصمانه را مورد بررسی قرار دادند. عدم امنیت نیروی انسانی که تا حدودی ناشی از تغییرات آب و هوا و شرایط محیطی می‌باشد، ممکن است منجر به مشکلات امنیتی بزرگتر و وخیم‌تری برای سازمان گردد (۱۶). Gutiérrez Vela و همکارانش در مطالعه‌ای به طراحی ساختاری جهت مدیریت کنترل دسترسی در سیستم‌های مشترک سازمانی، مبتنی بر مدل‌های سازمانی پرداختند که بر اساس آن مدیریت امنیت در سیستم‌های سازمانی کنونی یک فرآیند پیچیده است و بایستی همانند سایر جنبه‌های مهم سازمانی، در فرآیند توسعه مورد تحلیل قرار گیرد (۱۷). Da Veiga و Eloff در سال ۲۰۱۰ میلادی در مقاله‌ای بیان می‌کنند که رویکرد اطلاعاتی به امنیت اطلاعات، بایستی متمرکز بر رفتار کارکنان باشد، زیرا موفقیت و شکست سازمان به طور عمده‌ای مبتنی بر فعالیت‌هایی است که کارکنان انجام می‌دهند و یا در انجام آن‌ها با شکست مواجه می‌شوند (۱۸).

در پژوهش حاضر سعی بر آن شد تا به کمک استاندارد ISO/IEC 27001 میزان رعایت اصول امنیتی و به طور کلی وضعیت مدیریت امنیت اطلاعات در بخش‌های فناوری اطلاعات دانشگاه علوم پزشکی اصفهان مورد ارزیابی قرار گیرد.

روش بررسی

این پژوهش کاربردی و از دسته مطالعات توصیفی-کیفی است. جامعه پژوهش کلیه بخش‌های فناوری اطلاعات دانشگاه علوم پزشکی اصفهان از جمله مراکز کامپیوتر دانشکده‌ها (۹ مرکز)، بیمارستان‌ها (۱۳ مرکز) و مرکز آمار و اطلاع رسانی دانشگاه (جمعا ۲۳ مرکز) در سال ۱۳۹۰ خورشیدی، می‌باشد. دانشگاه علوم پزشکی و خدمات درمانی استان اصفهان یکی از دانشگاه‌های دولتی ایران و تحت پوشش وزارت بهداشت، درمان و آموزش پزشکی است که در سال ۱۳۲۵ خورشیدی تأسیس شد. از میان ۷ حوزه معاونت، معاونت پشتیبانی دانشگاه تحت نظارت مستقیم رئیس دانشگاه، امور رفاهی، فنی، مالی، خدمات پشتیبانی، آمار و اطلاع‌رسانی، توسعه سازمان و منابع سازمان، بهره وری، و ... را مدیریت می‌نماید. مرکز آمار و اطلاع‌رسانی از جمله بخش‌های مدیریتی زیرمجموعه معاونت پشتیبانی دانشگاه است که با نظارت معاون پشتیبانی در حال فعالیت می‌باشد.

ابزار گردآوری در این پژوهش استاندارد ISO/IEC 27001: 2005 می‌باشد که در قالب چک‌لیست بین المللی ارائه شده

است (۱۹). این استاندارد بین‌المللی به منظور ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات سازمان تهیه شده و دیدگاه فرآیندگرا را بر می‌گزیند. چک لیست مورد استفاده دارای ۱۱ بخش اصلی است، که هر کدام در برگیرنده چندین بخش فرعی و سؤال می‌باشد.

با توجه به اینکه ابزار مورد استفاده در این پژوهش توسط متخصصین حوزه‌های مربوطه در سازمان بین المللی و معتبر ISO به منظور فرآیندهای ممیزی پیشنهاد گردیده و مقیاسی استاندارد می‌باشد، و همچنین با توجه به نظرات کارشناسی اساتید حوزه فناوری اطلاعات در مورد این استاندارد و قابلیت اجرای کامل آن در سازمان‌های کشورمان، روایی و پایایی آن تأیید شده می‌باشد. داده‌ها از طریق مصاحبه با مدیریت ارشد مرکز آمار و اطلاع‌رسانی دانشگاه علوم پزشکی اصفهان و معاونین وی (۴ نفر) و همچنین مشاهده و مستندات پژوهشگران، گردآوری و وارد چک لیست گردید. پس از گردآوری داده‌ها، به هر یک از آیتم‌ها بر اساس امتیازدهی لیکرت (از ۱ تا ۵) امتیازی داده شد. سپس تجزیه و تحلیل داده‌ها به کمک نرم‌افزار Excel ۲۰۱۰ انجام شد.

یافته‌ها

میزان اجرای بخش‌های فرعی و اصلی استاندارد ISO/IEC 27001 در سازمان در جدول ۱، میزان اجرای بخش‌های اصلی استاندارد ISO/IEC 27001 در سازمان در نمودار ۱ و میزان اجرای بخش‌های اصلی استانداردISO/IEC 27001 نسبت به میزان کلی اجرای استانداردISO/IEC 27001 در سازمان در نمودار ۲، نشان داده شده است.

همانگونه که در نمودار ۱ نشان داده شده است، سازمان در بخش امنیت محیطی و فیزیکی با ۷۳ درصد و در بخش سیاست امنیتی با ۳۱ درصد به ترتیب بیشترین و کمترین میزان اجرای استاندارد ISO/IES 27001 را داشته است.

در نمودار ۲، در کنار میزان اجرای بخش‌های اصلی استاندارد ISO/IEC 27001، میزان کلی اجرای استاندارد ISO/IEC 27001 در سازمان، به میزان ۵۲ درصد، با خط‌چین نشان داده شده است.

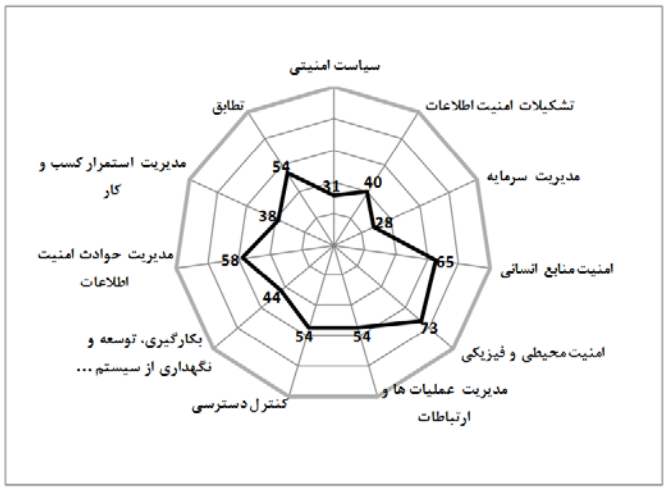
در این میان، میزان اجرای بخش‌های سیاست امنیتی، تشکیلات امنیت اطلاعات، مدیریت سرمایه، بکارگیری، توسعه و نگهداری از سیستم‌های اطلاعاتی و مدیریت استمرار کسب و کار کمتر از میزان کلی اجرای استاندارد و بخش‌های امنیت منابع انسانی، امنیت محیطی و فیزیکی، مدیریت عملیات‌ها و ارتباطات، کنترل دسترسی، مدیریت حوادث امنیت اطلاعات و تطابق بیشتر از میزان کلی اجرای استاندارد در سازمان می‌باشد.

جدول ۱: میزان اجرای بخش‌های فرعی و اصلی استاندارد ISO/IEC 27001 در سازمان

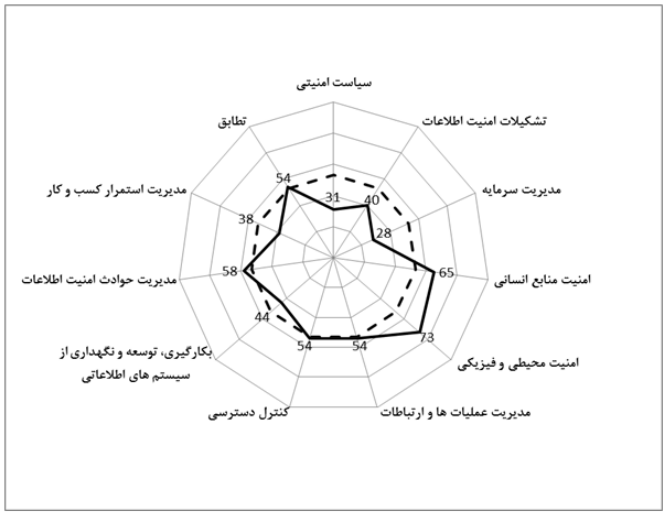
بخش‌های اصلی	بخش‌های فرعی	میزان خام	میزان اجرای استاندارد بر حسب درصد	
سیاست امنیتی	سیاست امنیت اطلاعات	۱۱	۳۱	۳۱
تشکیلات امنیت اطلاعات	سازمان داخلی	۱۶	۴۰	۴۰
	طرفین بیرونی	۶	۴۰	
مدیریت سرمایه	مسئولیت سرمایه ها	۴	۲۶,۶۷	۲۸
	دسته بندی اطلاعات	۳	۳۰	
امنیت منابع انسانی	قبل از استخدام	۲۲	۷۳	۶۵
	در حین استخدام	۴	۲۶,۶۷	
	پایان یا تغییر در استخدام	۱۳	۸۶,۶۷	

ادامه جدول ۱: میزان اجرای بخش‌های فرعی و اصلی استاندارد ISO/IEC 27001 در سازمان

بخش‌های اصلی	بخش‌های فرعی	میزان خام	میزان اجرای استاندارد بر حسب درصد	
امنیت محیطی و فیزیکی	مناطق امن	۲۸	۸۰	۷۳
	تجهیزات امنیتی	۴۵	۶۹	
مدیریت عملیات ها و ارتباطات	رویه های عملیاتی و مسئولیت ها	۱۴	۵۶	۵۴
	مدیریت ارائه ی خدمات شخص ثالث	۱۲	۴۸	
	سیستم برنامه ریزی و پذیرش	۹	۶۰	
	محافظت در برابر کدها مخرب و سیار	۱۵	۷۵	
	پشتیبان گیری	۹	۹۰	
	مدیریت امنیت شبکه	۱۸	۹۰	
	مدیریت رسانه ها	۱۰	۳۳	
	تبادل اطلاعات	۲۳	۶۵,۷۱	
	خدمات تجارت الکترونیک	۶	۲۸	
	کنترل و تنظیم	۲۳	۴۱,۸۲	
کنترل دسترسی	الزامات کسب و کار برای کنترل دسترسی	۸	۵۳	۵۴
	مدیریت دسترسی کاربر	۱۱	۴۴	
	مسئولیت های کاربران	۸	۴۰	
	کنترل دسترسی به شبکه	۴۲	۷۶	
	کنترل دسترسی به سیستم عملیاتی	۲۴	۶۰	
	کنترل دسترسی به اطلاعات و برنامه های کاربردی	۳	۳۰	
	محاسبه ی متغیر و کار از راه دور	۵	۲۵	
	الزامات امنیتی سیستم های اطلاعاتی	۶	۴۰	
بکارگیری، توسعه و نگهداری از سیستم‌های اطلاعاتی	پردازش صحیح در برنامه های کاربردی	۱۶	۴۸/۵۷	۴۴
	امنیت فایل های سیستم	۷	۳۵	
	امنیت در فرآیند توسعه و پشتیبانی	۲۳	۵۱	
	مدیریت آسیب پذیری فنی	۲	۲۰	
مدیریت حوادث امنیت اطلاعات	گزارش ضعف ها و حوادث مربوط به امنیت اطلاعات	۱۱	۷۳	۵۸
	مدیریت حوادث امنیت اطلاعات و بهبودها	۲۱	۵۲/۵	
مدیریت استمرار کسب و کار	جنبه های امنیت اطلاعات در مدیریت استمرار کسب و کار	۱۹	۳۸	۳۸
تطابق	تطابق با نیازهای قانونی	۳۹	۶۵	۵۴
	تطابق با سیاست های امنیتی و استانداردها و تطابق فنی	۱۱	۵۵	
	ملاحظات ممیزی سیستم های اطلاعاتی	۴	۲۰	



نمودار ۱: میزان اجرای بخش‌های اصلی استاندارد ISO/IEC 27001 در سازمان



نمودار ۲: میزان اجرای بخش‌های اصلی استاندارد ISO/IEC 27001 نسبت به میزان کلی اجرای استاندارد ISO/IEC 27001 در سازمان

بحث

ایجاد و پیاده‌سازی یک برنامه امنیت اطلاعات مناسب الزاماً کار بسیار دشواری نمی‌باشد و اجرای چنین برنامه‌ای بسیار بدیهی و معقول است (۱۷). بنابراین سازمان‌ها نیازمند یک چارچوب جامع جهت ایجاد و توسعه فرهنگ امنیتی در سرتاسر سازمان می‌باشند، که منجر به ایجاد فرهنگ امنیت اطلاعات در سازمان می‌شود (۲۰). در حیطه «سیاست امنیت»، سازمان توانسته است ۳۱ درصد از موارد خواسته شده توسط استاندارد را اجرا نماید. از آنجا که این بخش از حوزه‌های بسیار مهم مدیریت اثربخش سازمان در حوزه نگاه کلان به فناوری اطلاعات و مباحث مربوط به امنیت اطلاعات می‌باشد، می‌بایستی از طرف مدیران ارشد مورد توجه بیشتری قرار گیرد.Colwill در مطالعه‌ای معتقد است که کارکنان داخلی سازمان به واسطه در اختیار داشتن دسترسی قانونی به

بخش‌های مختلف، اطلاعات و دانش در خصوص سازمان و موقعیت دارایی‌های با ارزش آن، می‌توانند خطرات امنیتی بسیاری ایجاد نمایند و بایستی در راستای کاهش حملات داخلی در سازمان از سنجش‌ها و اقدامات پیشگیرانه استفاده نمود (۲۰). اما با توجه به این نکته، سازمان در حوزه «تشکیلات امنیت اطلاعات»، بین آیتم‌های موجود و میزان اجرای آن‌ها، تنها توانسته ۴۰ درصد از موارد را اجرایی نماید. از آنجا که اهم آیتم های این بخش در استاندارد، مربوط به تأمین امنیت قراردادهای شخص ثالث می‌باشد، اهمیت اجرای تمامی موارد آن از طرف سازمان با برنامه ریزی بلندمدت مدیران، نمود عینی بالایی دارد.

Anderson و Choobineh در سال ۲۰۰۸ میلادی اعلام کردند که با ظهور قابلیت‌های تبادل داده، شبکه‌های اشتراکی، زیرساختارهای عمومی، صرفه‌جویی و بهبود عملکرد ناشی از توزیع الکترونیک اطلاعات، انواع جدیدی از دارایی‌های سازمانی ایجاد شده‌اند (۲۱). این در حالی است که در حیطه «مدیریت سرمایه»، سازمان ۲۸ درصد از موارد را توانسته اجرایی نماید. بنابراین با نگاهی به موارد و آیتم‌های این بخش می‌توان به این نتیجه مهم دست یافت که مدیریت سرمایه‌ها و اموال سازمان چه از لحاظ مادی و چه حق معنوی برخی ار نرم افزارها می‌بایستی مورد دقت بیشتری قرار گیرد.

رویکرد اطلاعاتی به امنیت اطلاعات، بایستی متمرکز بر رفتار کارکنان باشد، زیرا موفقیت و شکست سازمان به طور عمده‌ای مبتنی بر فعالیت هایی است که کارکنان انجام می‌دهند. ایجاد فرهنگ آگاهی از امنیت اطلاعات باعث به حداقل رساندن ریسک‌های تهدیدکننده دارایی‌های اطلاعاتی و به ویژه کاهش خطرات ناشی از سوءرفتار و تعامل نامناسب کارکنان با دارایی‌های اطلاعاتی سازمان می‌گردد (۱۸). در این راستا و در حیطه «امنیت منابع انسانی»، سازمان بهتر از حیطه‌های دیگر ظاهر شده و توانسته است بر اساس امتیازدهی به نتایج مستندات و مشاهدات، ۶۵ درصد از موارد را اجرایی نماید. لذا می‌توان گفت در سازمان مباحثی همچون امنیت در حین استخدام، پس از استخدام و در حین اخراج و یا اتمام کار، به درستی مورد توجه قرار گرفته است تا منابع انسانی مؤثر در فرآیند امنیت اطلاعات، به شکل صحیح و به موقع اطلاعات را تحویل سازمان دهند.

Crossler و همکارانش معتقد هستند حوزه امنیت اطلاعات بسیار گسترده و شامل رویکردهای بسیاری جهت حفاظت از دارایی‌های اطلاعاتی و منابع تکنیکی موجود در سیستم‌های کامپیوتری و کاهش خطرات تهدیدکننده آن‌ها می‌باشد (۲۲). بنابراین امروزه تغییر آب و هوا و شرایط محیطی به عنوان یک مشکل امنیتی در نظر گرفته می‌شود (۱۶). در مطالعه حاضر عملکرد سازمان در حیطه «امنیت محیطی و فیزیکی» در سطح مناسبی بوده و توانسته است با بکارگیری موارد مهم امنیت محیطی و فیزیکی در مناطق مهم و استراتژیک، به میزان ۷۳ درصد آیتم‌های موجود را اجرایی نماید.

یکی از اولویت‌های عمده و مهم در سازمان بایستی بر کارکنان و مستندات و قوانینی جهت ارزیابی خطرات امنیتی متمرکز باشد (۱۸). Boudaoud و همکارانش در مطالعه‌ای در سال ۲۰۰۰ میلادی اعلام کردند که تعداد کاربران استفاده کننده از شبکه به سرعت در حال افزایش است و در این شرایط، شبکه‌های خصوصی و سازمانی در معرض تهدید حمله‌های شرورانه قرار دارند (۲۳). با در نظر گرفتن این نکات، در حیطه «مدیریت عملیات‌ها و ارتباطات»، سازمان تنها ۵۴ درصد از موارد موجود در استاندارد را اجرایی نموده است. از آنجا که این بخش موارد مهمی همچون مدیریت تغییرات، مدیریت ظرفیت، کنترل کدهای مخرب و ... را مورد لحاظ قرار می‌دهد، مدیران ارشد سازمان می‌بایستی توجه بیشتری را به اجرا نمودن آن معطوف نمایند.

یکی از مهم‌ترین مشخصه‌های سیستم‌های سازمانی کنونی، وجود فرآیندهای مشترک در راستای انجام فعالیت‌های روتین سازمان می‌باشد که در این فرآیندها، به طور معمول منابع مشترک مورد استفاده قرار گرفته است. در نتیجه تعریف و اجرای سطوح امنیتی مختلف (در زمینه اقدامات، کاربران، منابع و...) ضروری است (۱۵). در مطالعه حاضر، سازمان در حیطه «کنترل دسترسی»، نیز از مجموع موارد و آیتم‌ها تنها

توانسته ۵۴ درصد را اجرایی نماید. به دلیل اهمیت نقش کنترل دسترسی در محیطهای مختلف سازمان‌های فناوری اطلاعات، در راستای بالا بردن سطح امنیت، می‌بایستی سازمان کمیته‌ای در این خصوص ایجاد نموده تا با ارائه راهکارهایی در کوتاه مدت و همچنین برنامه‌ریزی بلندمدت برای استقرار آن‌ها، بتوانند تمام آیتم‌های مورد اشاره استاندارد را در این حوزه اجرایی نمایند.

Mellado و Fernández-Medina در مطالعه‌ای در سال ۲۰۰۷ میلادی اعلام می‌کنند که در راستای ایجاد و توسعه سیستم‌های اطلاعاتی بحرانی در سازمان، تعیین نیازمندی‌های کیفیت امنیت بسیار با اهمیت و در عین حال بسیار دشوار می‌باشد (۱۴). با توجه به این موضوع، در حیطه «بکارگیری، توسعه و نگهداری از سیستم‌های اطلاعاتی» که مواردی همچون کنترل پردازش داخلی، اعتبار داده‌های ورودی، یکپارچگی پیام‌ها، اعتبار داده‌های خروجی و موارد کنترلی دیگر را در بر می‌گیرد، سازمان تنها توانسته ۴۴ درصد از موارد را اجرا نموده و در این بخش بسیار ضعیف می‌باشد.

Colwill معتقد است راه حل‌ها بایستی سریعاً طراحی و پیاده‌سازی شده و باعث ایجاد و حفظ اعتماد و روابط ایمن در طی زمان شوند. او همچنین بیان می‌کند بایستی در راستای کاهش حملات در سازمان از سنجش‌ها و اقدامات پیشگیرانه استفاده نمود و نباید تنها پس از وقوع حوادث امنیتی به فکر راه حلی جهت حل مشکل افتاد (۲۰). در این مطالعه، در حیطه «مدیریت حوادث و نگهداری از سیستم‌های اطلاعاتی»، ۵۸ درصد از موارد در سازمان اجرایی گردیده و همانطور که قبلا در حیطه امنیت محیط فیزیکی بدان اشاره شد، خط مشی‌های خوبی در این زمینه در سازمان تدوین گردیده است که می‌توان با بروزرسانی آن‌ها بر اساس نیاز تمامی بخش‌ها و همچنین استفاده از فناوری‌های جدید جخانی در این حوزه، عدد آن را مورد ارتقا قرار داد.

Quirchmayr در سال ۲۰۰۴ میلادی اعلام می‌کند که فرآیند کسب و کار و رفتار سازمانی مناسب در رابطه با امنیت و مدیریت استمرار کسب و کار، قدم اولیه و بسیار مهمی در راستای بهبود وضعیت امنیت سازمان می‌باشد (۲۴). مدیران سازمان مورد نظر در این مطالعه دارای نگاه کلانی در رابطه با حیطه «مدیریت استمرار کسب و کار» می‌باشند، اما در حال حاضر در حدود ۳۸ درصد از موارد مورد نظر استاندارد اجرایی گردیده‌اند.

Kanno، محقق ژاپنی، دلیل پرطرفدار بودن بهبودهای تطبیقی سنجش امنیت اطلاعات در ژاپن را تطابق با استاندارد بین المللی، استفاده رایگان از استاندارد و... را عنوان می‌کند (۲۵). با توجه به این نکته، در حیطه «تطابق» که موارد مهمی همچون محافظت از ابزارهای ارزیابی، ممیزی‌ها، زمانبندی برای اجرای آن‌ها و ... را در بر می‌گیرد، سازمان مورد مطالعه توانسته است ۵۴ درصد از موارد را جامه عمل پوشاند. از محدودیت‌های این پروژه می‌توان به مواردی همچون عدم همکاری مسؤولین مرکز آمار و اطلاع رسانی دانشگاه در برگزاری جلسات و ارائه اطلاعات، عدم ارائه بخشی از اطلاعات جمع‌آوری شده در گزارش نهایی، به دلیل عدم تأیید آن‌ها از جانب مسؤولین مربوطه، محرمانگی و حساسیت بالای اطلاعاتی که باید در این پژوهش مورد گردآوری قرار می‌گرفتند، لزوم تأیید انجام پروژه از جانب حراست و معاونت پشتیبانی دانشگاه علوم پزشکی اصفهان و همچنین مراجع قانونی بالاتر، طولانی شدن فرآیندهای هماهنگی‌های تشکیل جلسات به دلیل عدم همکاری مراجع ذیربط و طولانی شدن بازه ی زمانی انجام پروژه، اشاره نمود.

نتیجه‌گیری

با توجه به اینکه عصر حاضر عصر اطلاعات نام دارد و در تمامی سازمان‌های فعال در جامعه بطور مداوم حجم وسیعی از اطلاعات تولید و مبادله می‌شود، اجرای مطالعاتی نظیر پژوهش حاضر به مدیران سازمان‌ها کمک می‌کند تا سیاست‌های صحیحی را در زمینه امنیت اطلاعات سازمان خود، در کلیه حیطه‌ها، تدوین و اجرا نمایند. به منظور پیاده‌سازی امنیت کامل و مناسب اطلاعاتی در جامعه بهتر است در سازمان‌های مختلف گروه‌هایی از افراد متخصص در زمینه امنیت اطلاعات تشکیل گردیده و بطور دوره‌ای و به

کمک ابزارهای مناسب میزان امنیت اطلاعات سازمان را مورد ارزیابی قرار داده و نتایج حاصله را جهت رفع نقوص به مدیریت گزارش نمایند. یافته‌های این پژوهش با ارائه تصویری روشن از وضعیت امنیت اطلاعات، به افراد مسؤول در سازمان مورد مطالعه کمک می‌کند تا نقاط آسیب‌پذیر را شناسایی نموده و به منظور رفع کاستی‌های موجود سیاست‌های امنیتی مناسب با اهداف سازمان را طراحی و اجرا نمایند.

پیشنهادها

– پیشنهاد می‌گردد مدیران ارشد سازمان پس از جستجو در شرکت‌های طراح امنیت، گروهی را برای طراحی سیاست امنیت اطلاعات در سازمان خود انتخاب نمایند. سازمان در این خصوص می‌تواند از اعضای هیأت علمی و دانشجویان خود دانشگاه که در ارتباط با حوزه IT و امنیت اطلاعات تحقیقاتی دارند دعوت به انجام کار نماید.

– پیشنهاد می‌گردد تمامی دارایی‌های شناسایی شده سازمان دارای مالک بوده و محدودیت‌های دسترسی به آن‌ها مستند گردد.

– پیشنهاد می‌گردد تمامی مسؤولیت‌ها و وظایف امنیتی کارمندان، پیمانکاران و مصرف‌کنندگان با توجه به سیاست امنیتی سازمان به طور واضح و آشکاری مستند گردیده و پس از تأیید مدیریت ارشد به ایشان ابلاغ گردد.

– پیشنهاد می‌گردد دستورالعملی به منظور مدیریت تغییرات کل سازمان در حوزه‌های سخت‌افزار و نرم‌افزار و شبکه و ارتباطات بیرونی، به همراه شناسایی دقیق نقاط پر ریسک کسب و کار سازمان، تدوین گردیده و پس از تأیید و تصویب مدیریت ارشد به اجرا در آید.

– پیشنهاد می‌گردد که دستورالعملی جامع که در برگیرنده تمامی مشتریان بیرونی و داخلی سازمان (بیماران، کارمندان بیمارستان، کارمندان دانشگاه، دانشجویان، استادان، مدیران ارشد، پیمانکاران و ...) می‌باشد تدوین گردیده و به محض ورود یک مشتری به سازمان براساس روش‌های شناسایی که در دستورالعمل قید گردیده است ارتباط مشتری با سیستم‌های اطلاعاتی و شبکه سازمان برقرار گردد.

– پیشنهاد می‌گردد که دوره‌های آموزشی در خصوص امنیت اطلاعات برای کلیه افراد مرتبط با سازمان برگزار گردیده و برای شرکت در این دوره‌ها الزام ایجاد شود

– پیشنهاد می‌گردد بخش آموزش سازمان نیازسنجی آموزشی پرسنل و مصرف کنندگان را انجام داده و همچنین پس از برگزاری آموزش اثربخشی آموزشی آن‌را مورد ارزیابی قرار دهد.

References

1. Ghasemi K, Mokhtari V, Amini M. Security and electronic commerce. Proceeding of the fourth national conference of electronic commerce, 2007; Tehran.
2. Safayi A. Management information systems. Tehran: Jaber Farmacy Corporation; 2011.
3. Farhadi R. Information technology and communication fundamentals. Tehran: Ketabdar; 2011.
4. Zirack M. Information Management Systems (MIS) Role on University's organizational culture elements. [On Line]. 2012. Available from: URL:http://vista.ir/article/258187.
5. Kankanhalli A, Teo HH, Tan BC, Wei KK. An integrative study of information systems security effectiveness. International Journal of Information Management 2003; 23(2): 139-54.
6. Sheikhpour R, Modiri N. An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls. International Journal of Security and Its Applications 2012; 6(2): 13-28.
7. Nakhaeai H. Introduction to information security management system. [On Line]. 2012. Available from: URL: http://vista.ir/article/355.
8. Farn KJ, Lin SK, Fung ARW. A study on information security management system evaluation-assets, threat and vulnerability. Computer Standards & Interfaces 2004; 26(6): 501-13.
9. Siponen M, Willison R. Information security management standards: Problems and solutions. Information & Management 2009; 46(5): 267-70.
10. Khorasani A, Hosein abadi H, Amirzadeh R. ISO/IEC 27001: 2005 Standard. Tehran: Kiyarash; 2006.
11. Abedian S, Bitaraf A. Presentation of hospital information system evaluation model in Iran. Tehran: Information technology and statistical center of department of health and medical education; 2012.

12. Sedighiyani A. Evaluation of health care and hospital standards. Tehran: Jafary; 2005.[In Persian]
13. Kakkar A, Punhani R, Madan S. Implementation of ISMS and its practical shortcomings. International research journal 2012; 2(1):2-7.
14. Mellado D, Fernández-Medina E, Piattini M. Common criteria based security requirements engineering process for the development of secure information systems. Computer standards & interfaces 2007; 29(2): 244-53.
15. Von Solms B, Von Solms R. The 10 deadly sins of information security management. Computers & Security 2004; 23(5): 371-6.
16. Barnett J, Adger WN. Climate change, human security and violent conflict. Political Geography 2007; 26(6): 639-55.
17. Gutiérrez Vela FL, Isla Montes JL, Paderewski Rodríguez P, Sanchez Roman M, Jiménez Valverde B. Architecture for access control management in collaborative enterprise systems based on organization models. Science of Computer Programming 2007; 66(1): 44-59.
18. Da Veiga A, Eloff JH. A framework and assessment instrument for information security culture. Computers & Security 2010; 29(2): 196-207.
19. Val Thiagarajan BE. BS ISO/IEC 17799:2005 (BS ISO/IEC 27001:2005) BS 7799-1:2005, BS 7799-2: 2005 SANS Audit Checklist. [On Line]. 2005. Available from: URL: https://www.sans.org/media/score/checklists/ISO-17799-2005.pdf.
20. Colwill C. Human factors in information security: The insider threat–Who can you trust these days? Information security technical report 2009; 14(4): 186-96.
21. Anderson EE, Choobineh J. Enterprise information security strategies. Computers & Security 2008; 27(1): 22-9.
22. Crossler RE, Johnston AC, Lowry PB, Warkentin M, Baskerville R. Future directions for behavioral information security research. Computers & Security 2013; 32: 90-101.
23. Boudaoud K, Labiod H, Boutaba R, Guessoum Z. Network security management with intelligent agents. Network Operations and Management Symposium 2000. United States: IEEE/IFIP; 2000.
24. Quirchmayr G. Survivability and business continuity management. Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalization; 2004. Australia: Australian Computer Society Inc, 2004 .
25. Kanno Y, Terada M, Yajima H. A comparative study on structure of the motivation for information security by security incident experiences. Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human 2009. United States: ACM; 2009.

Evaluation of Information Management Systems in Isfahan University of Medical Science by ISO/IEC 27001 Standard*

Rouhollah Sheikh Abumasoudi[1], Sahar Koohi Habibi[2], Maryam Ataei[2], Nazila Esmaeili[2]

Original Article

Abstract

Introduction: considering the information threats and the need to procedures for develop and improve security and confidentiality, international standard organization (ISO) established information security standard ISO/IEC 27001. Getting ISO/IEC 27001 standard certificate helps the organization to identify the problems and defeats in its departments and processes, in addition to promoting organization's competitive position and giving the organization the competitive advantage that it needs. The goal of this study is to evaluate information management systems in Isfahan University of Medical Science using ISO/IEC 27001 standard.

Methods: This applied research is a descriptive study. Research community is all departments of information technology at Isfahan University of Medical Science, computer centers of faculties and hospitals, in 2011. In this research we used ISO/IEC 27001:2005 international checklist as a tool for collecting the information. The checklist includes 11 primary parts and each part includes several additional parts and questions. The information was gathered through interviewing, observation and documents of researchers and was analyzed by Excel 2010.

Results: the assessment results indicates that in standard main parts including security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information system acquisitions, development and maintenance, information security incident management, business continuity management and compliance, the organizations implemented 31, 40, 28, 65, 73, 54, 54, 44, 58, 38 and 54 percent of the requirements.

Conclusion: considering the importance of developing information security management in organizations that deliver information technology services and also the importance of international standard ISO/IEC 27001 in establishing the organization's processes based on information security and confidentiality protection, integrity and accessibility, the organization should put more effort into implementing this standard in its processes. The results indicate that except for the human resources security and physical and environmental security areas, the organization didn't develop information security management requirements properly in its internal processes.

Keywords: Evaluation; Management Information Systems; Standards.

Received: 24 Nov, 2014 Accepted: 5 Jan, 2015

Citation: Sheikh Abumasoudi R, Koohi Habibi S, Ataei M, Esmaeili N. **Evaluation of Information Management Systems in Isfahan University of Medical Science by ISO/IEC 27001 Standard.** Health Inf Manage 2015; 12(3):316.

*- This article was resulted from Project no 290107 supported by Isfahan University of Medical sciences.

1- Lecturer, Industrial engineering, Isfahan University of Medical sciences, Isfahan, Iran (Corresponding Author) Email: abumasoudi@live.com

2- BSc, Health Information Technology, Isfahan University of Medical sciences, Isfahan, Iran