بررسی و تحلیل تغییرات استاندارد ISO/IEC 27001: 2013 و ارائه مدل انتقال

مصطفی تمتاجی
طاهره رضایی

تاریخ دریافت: ۹۳/۲/۷
تاریخ پذیرش: ۹۳/۲/۲۴

چکیده:

تداوم کسب‌وکار یک سازمان و بقای آن در عرصه‌ی رقابت، در گرو موفقیت در حفظ امنیت اطلاعات حیاتی خود و ذی‌نفعان است. استاندارد ISO/IEC 27001 برای نخستین بار در سال ۲۰۰۵ مجموعه‌ای از کنترل‌های امنیتی فیزیکی، مدیریتی و فنی را یکجا جمع کرد و به‌عنوان نظام مدیریت امنیت اطلاعات منتشر شد. در سال ۲۰۱۳ تجربیات موفق و ناموفق سازمان‌ها در ایجاد امنیت اطلاعات و ارتقای واقعی سطح امنیتی با بهره‌گیری از این استاندارد منجر به انتشار ویرایش جدیدی از آن گردید.

در این مقاله، با دانسته فرض کردن الزامات استاندارد ویرایش سال ۲۰۰۵، تغییرات کلی ویرایش سال ۲۰۱۳ مرور خواهد شد. همچنین مدل عملیاتی برای انطباق نظام‌های استقرار یافته براساس استاندارد ویرایش ۲۰۰۵ به ویرایش ۲۰۱۳ ارائه خواهد شد.

واژگان کلیدی:

نظام مدیریت امنیت اطلاعات، استاندارد، کنترل‌های امنیت اطلاعات

۱) مقدمه

با افزایش روزافزون وابستگی سازمان‌ها به فناوری اطلاعات، دغدغه‌های امنیتی این حوزه گسترش یافته و به چالش جدی مدیران و متخصصین تبدیل شده است. برآورده شدن الزامات امنیتی به‌صورت کامل و مطمئن مستلزم نگاهی کلان و همه‌جانبه به مبحث امنیت اطلاعات است تا از این طریق بتوان لایه‌ها و سطوح مختلف درگیر در امنیت مانند حوزه‌های مدیریتی، عملیاتی، فیزیکی، فنی و منابع انسانی را پوشش داد.

نظام مدیریت امنیت اطلاعات مبتنی براساس استاندارد بین‌المللی ISO/IEC 27001 با چنین دیدگاهی در سازمان‌ها طراحی و عملیاتی می‌شود.

این استاندارد بیان می‌کند که هر سازمانی برای سه رأس مثلث امنیت اطلاعات[1] (ایجاد و حفظ محرمانگی، صحت و یکپارچگی و دسترس‌پذیری اطلاعات)، باید نظام مدیریت امنیت اطلاعات را به‌عنوان یک روش پیشگیرانه، طراحی و پیاده‌سازی نماید. این اطلاعات می‌تواند شامل اطلاعات سازمان، مشتریان و یا اشخاص ثالث باشد. نکته‌ی مهم در بقا و ماندگاری یک سازمان این است که بتواند نیازهای ذی‌نفعان را طوری سامان دهد که امنیت اطلاعات آن‌ها خدشه‌دار نشود .

این استاندارد توسط کمیته فنی مشترک فناوری اطلاعات (JTC۱) نخستین بار در سال ۲۰۰۵ منتشر شد و پس از تحلیل تجربیات به‌دست آمده از استقرار

1. Confidentiality, Integrity, Availability- CIA

آن در سازمان‌ها، در سال ۲۰۱۳ ویرایش جدید آن منتشر شد. در واقع، براساس تحقیقاتی که در اوایل سال ۲۰۱۳ توسط PWC[1] به نیابت از بخش تجارت انگلستان منتشر شد، نتایجی بیان شده است که طبق آن کسب‌وکارهای کوچک، سطوح مختلفی از حوادثی را تجربه کرده بودند که پیشتر تنها در سازمان‌های بزرگ رویت شده بود؛ همچنین در سال گذشته ۸۷ درصد از سازمان‌های کوچک نیز رخنه امنیتی گزارش کرده بودند.

علاوه‌بر آن، این گزارش بیانگر تأثیر افزایش روزافزون استفاده از فناوری‌های جدید و نیز رخنه‌های امنیتی است که از طریق شبکه‌های اجتماعی، تلفن‌های هوشمند و تبلت‌ها اتفاق می‌افتند.

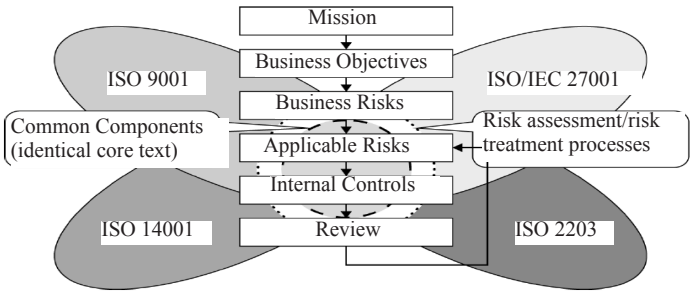
از طرفی انتظار می‌رود ویرایش جدید استاندارد، منعکس‌کننده‌ی تغییراتی باشد که Edward Humphries در جلسه کارگروه مسئول تدوین و حفظ این استاندارد اعلام داشت: "ما پیشرفت‌هایی را در زمینه کنترل‌های امنیتی داشته‌ایم که در پیوست A این استاندارد ذکر شده‌اند تا تضمین کننده روزآمدی استانداردها بوده و می‌توانند با مخاطرات زندگی امروز از جمله سرقت هویت، مخاطرات مربوط به تجهیزات سیار و دیگر آسیب‌پذیری‌های آنلاین، مقابله نمایند."

درحال حاضر طبق آمار بین‌المللی بیش از ۱۷۰۰۰ سازمان در سراسر جهان ثبت شده است که نظام مدیریت امنیت اطلاعات[2] را براساس استاندارد ISO/IEC27001:2005 استقرار داده‌اند که لازم است ISMS خود را با الزامات ویرایش جدید استاندارد تطبیق دهند [4,5].

در این مقاله تغییرات نسخه جدید استاندارد بررسی شده و ساختار دو استاندارد با یکدیگر مورد مقایسه قرار گرفته‌اند. درنهایت با توجه به اینکه سازمان‌ها موظف به استقرار استاندارد براساس ویرایش جدید آن هستند، مسیر و مدل‌گذار از ویرایش قبلی به ویرایش جدید بیان خواهد شد. هدف این مقاله تنها مرور و مقایسه‌ی تغییرات و ارائه‌ی گام‌های عملیاتی برای استقرار ویرایش جدید استاندارد برای سازمان‌هایی که ویرایش قبلی را استقرار داده‌اند، بوده و به محتوای استاندارد و موارد مشترک دو ویرایش و ارائه مدل استقرار آن برای سازمان‌هایی که برای نخستین بار به استقرار ISMS رو آورده‌اند، نخواهد پرداخت.

۲) مقایسه‌ی ISO/IEC27001:2013 با ISO/IEC27001:2005

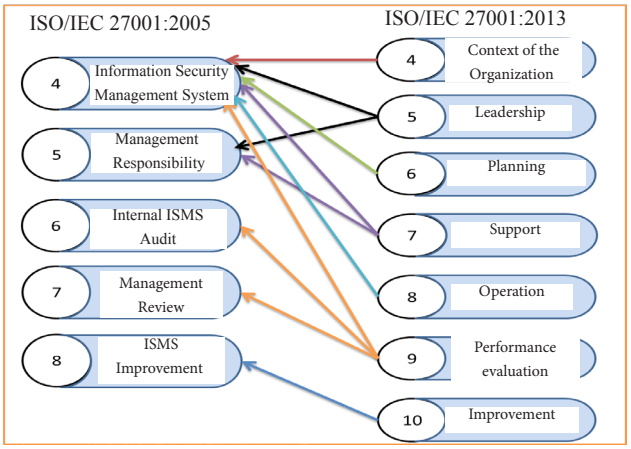
۱. از نقطه‌نظر ساختاری، متن استاندارد ویرایش جدید همراستا با ضمیمه‌ی SL از سری راهنماهای ISO تغییر کرده تا مطابق آنچه در شکل (۱) نشان داده شده است، با سایر استانداردهای مدیریتی منطبق باشد. دلیل این کار کمک به سازمان‌هایی است که بیش از یک استاندارد نظام مدیریت را به‌طور هم‌زمان اجرا می‌کنند، همچنین برای مراجع گواهی‌کننده و ممیزان سازمان‌هایی که بیش از یک استاندارد را استفاده می‌کنند، نیز مفید است [2,4,6,7].



شکل ۱: ساختار کلان و سازگاری استانداردهای نظام‌های مدیریتی مختلف

1. Price waterhouse Coopers
2. Information Security Management System: ISMS

بندهـای اصلـی کـه در اسـتانداردهای مدیریتـی وجـود دارنـد، عبارتنـد از: مقدمـه، دامنـه کاربـرد، مراجـع الزامـی، اصطلاحـات و تعاریـف، زمینـه سـازمان، رهبـری، طرح‌ریـزی، پشـتیبانی، عملیـات، ارزیابـی عملکـرد و بهبـود. شـکل (۲) سـاختار دو اسـتاندارد ویرایـش ۲۰۰۵ و ۲۰۱۳ را مقایسـه می‌کنـد [6,7].



شکل ۲: مقایسه ساختاری استاندارد ویرایش ۲۰۰۵ و ۲۰۱۳

۲. در ایـن ویرایـش نیـز ماننـد ویرایـش قبلـی، پیوسـت (الـف) حـاوی حوزه‌هـا و کنترل‌هـای امنیتـی اسـت بـا ایـن تفـاوت کـه تعـداد اهـداف کنترلـی و کنترل‌هـای امنیتـی از ۱۳۳ کنتـرل بـه ۱۱۴ کنتـرل کاهـش یافتـه و تعـداد حوزه‌هـای کنترلـی از ۱۱ حـوزه بـه ۱۴ حـوزه افزایـش یافتـه اسـت. در واقـع ارتبـاط بـا تأمین‌کننـدگان به‌عنـوان یـک دامنـه کنترلـی جدیـد مطـرح شـده اسـت. دامنـه کنترلـی ارتباطـات و مدیریـت عملیـات بـه دو دامنـه امنیـت عملیـات و امنیـت ارتباطـات تقسـیم شـده اسـت. رمزنـگاری یـک دامنـه کنترلـی جدیـد شـده اسـت و بخشـی از اکتسـاب سـامانه‌های اطلاعاتـی، توسـعه و نگهـداری نیسـت. جـدول (۱) فهرسـت حوزه‌هـای کنترلـی ویرایـش جدیـد را در مقایسـه بـا ویرایـش قبلـی بیـان می‌کند [1,2,7].

ISO/IEC 27001: 2005		ISO/IEC 27001: 2013	
5	Security policy	5	Information security policies
6	Organization of information security	6	Organization of information security
8	Human resources security	7	Human resource security
7	Asset management	8	Asset management
11	Access control	9	Access control
12	Information systems acquisition, development and maintenance(12.3 only)	10	Cryptography
9	Physical and environmental security	11	Physical and environmental security
10	Communications and operations management	12	Operations security
		13	Communications security
12	Information systems acquisition, development and maintenance	14	System acquisition, development and maintenance
	N/A	15	Supplier relationships
13	Information security incident management	16	Information security incident management
14	Business continuity management	17	Information security aspects of business continuity management
15	Compliance	18	Compliance

جدول ۱: مقایسه‌ی حوزه‌های کنترلی ویرایش ۲۰۰۵ و ۲۰۱۳

در مـورد تغییـرات کنترل‌هـا نیـز، برخـی کنترل‌هـا بـا هـم ادغـام شـده‌اند، برخـی حـذف یـا اضافـه شـده‌اند و تعـداد زیـادی از کنترل‌هـا بـه قـوت خـود باقـی هسـتند، البتـه ممکـن اسـت برخـی از کنترل‌هـا بـه حـوزه دیگـری منتقـل شـده باشـند. فهرسـت کنترل‌هـای حـذف شـده در ادامـه بیـان شـده‌اند: [1,2,7]

- 6-2-2: الزامات امنیتی در مواجهه با مشتریان
- 10-4-2: کنترل در برابر کدهای سیار
- 10-7-3: روش‌های اجرایی جابه‌جایی اطلاعات
- 10-7-4: امنیت مستندات ISMS
- 10-8-5: سامانه‌های اطلاعاتی کسب‌وکار
- 10-9-3: اطلاعات در دسترس عموم
- 11-4-2: تصدیق هویت کاربر برای ارتباطات خارجی
- 11-4-3: شناسایی تجهیزات در شبکه‌ها
- 11-4-4: محافظت از درگاه‌های پیکربندی و عیب‌یابی

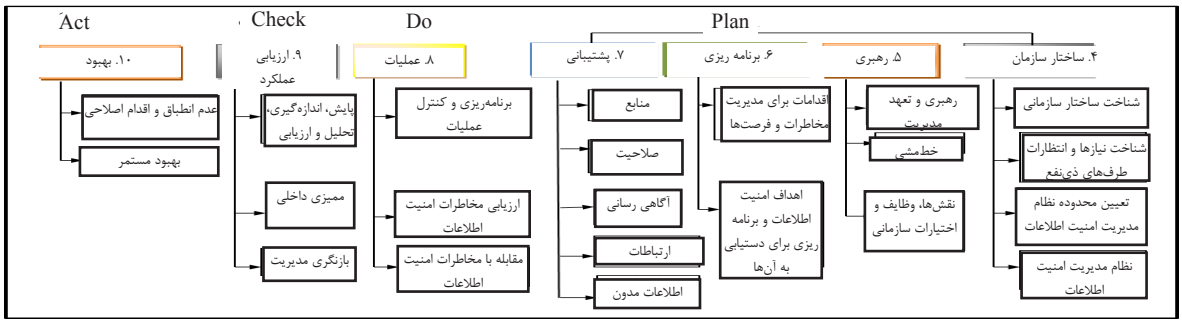
راه دور

- 11-4-6: کنترل ارتباط شبکه‌ها
- 11-4-7: کنترل مسیریابی شبکه
- 11-5-5: خاتمه مهلت استفاده از یک جلسه
- 11-5-6: محدودیت زمان اتصال
- 11-6-2: جداسازی سامانه‌های حساس
- 12-2-1: صحه‌گذاری داده‌های ورودی
- 12-2-2: کنترل پردازش داخلی
- 12-2-3: یکپارچگی پیام
- 12-2-4: صحه‌گذاری داده‌های خروجی
- 12-5-4: نشت اطلاعات
- 14-1-2: تداوم کسب و کار و ارزیابی مخاطرات
- 14-1-3 : توسعه و پیاده‌سازی طرح‌های تداوم کسب‌وکار
- 14-1-4: چارچوب طرح تداوم کسب‌وکار
- 15-1-5: جلوگیری از سوء استفاده از امکانات پردازش اطلاعات
- 15-3-2: حفاظت از ابزارهای ممیزی سامانه‌های اطلاعاتی

در ایـن نسـخه کنترل‌هـا به‌صورتـی ذکـر شـده‌اند کـه آزادی عمـل بیشـتری را بـرای انتخـاب روش پیاده‌سـازی نظـام مدیریـت امنیـت اطلاعـات بـه کارشناسـان می‌دهنـد و بـا معرفـی یـک روش بـرای مقابلـه بـا مخاطـرات[1] کارشناسـان را در انتخـاب خط‌مشـی‌های امنیتـی صحیـح یـاری می‌دهنـد.

اسـتاندارد تصریـح می‌کنـد کـه کنترل‌هـا قـرار نیسـت از پیوسـت (الـف) انتخـاب شـوند، بلکـه مسـتقیماً در فراینـد مدیریـت مخاطـرات گزینـش می‌شـوند. بـا ایـن حـال می‌تـوان از ایـن پیوسـت بـرای اطمینـان از اینکـه کنترل‌هـای ضـروری فرامـوش نشـده‌اند، اسـتفاده کـرد.

۳. چرخـه PDCA کـه مبنـای عملکـرد نظـام مدیریـت امنیـت اطلاعـات در بخـش بهبـود مـداوم بـود، در نـگارش جدیـد اجبـاری نیسـت و می‌توانـد بـا روش‌هـای دیگـری جایگزیـن شـود. گرچـه تأکیـد بـر چرخـه PDCA در ایـن اسـتاندارد حـذف شـده اسـت، لیکـن مطابـق بـا سـاختار ارائـه شـده در شـکل (۳) مشـخص اسـت کـه مفاهیـم ایـن چرخـه در متـن اسـتاندارد وجـود دارد. از دلایـل ایـن تغییـر نگـرش، می‌تـوان بـه ارتقـای سـطح دانـش سـازمان اشـاره کـرد کـه انتظـار مـی‌رود سـازمان‌ها قـادر باشـند مفاهیـم پایـه‌ای را در حیـن اجـرای هـر فراینـدی لحـاظ نماینـد [7].



شکل ۳: ساختار متن استاندارد ISO/IEC 27001:2013

1. Risk Treatment

۴. مفاهیم مستندات و سوابق با هم ادغام شده و مفهوم اطلاعات مدون را ایجاد کرده است. بنابراین تمام الزاماتی که برای کنترل مستندات وجود داشت، اکنون برای مستندات و سوابق، الزامی است لیکن الزام برای وجود رویه‌های مستند مانند کنترل مستندات، ممیزی داخلی، اقدامات اصلاحی و پیشگیرانه حذف شده است. اگرچه الزام مدون نمودن خروجی این رویه‌ها در استاندارد جدید کماکان وجود دارد. جدول پیوست (الف) فهرست مستندات الزامی و اختیاری را براساس ویرایش جدید استاندارد بیان می‌کند [1,2,3].

۵. شناسایی دارایی‌ها، تهدیدات و آسیب‌پذیری‌ها دیگر مبنای ارزیابی مخاطرات نیست و روش‌شناسی مدیریت مخاطرات می‌تواند براساس نیاز سازمان انتخاب شود. این موارد صرفاً برای تعیین مخاطرات مرتبط با محرمانگی، تمامیت و دسترس‌پذیری مورد نیاز بوده و دیگر پیش‌نیاز شناسایی مخاطرات نیستند [1,2,3].

۶. در ویرایش جدید استاندارد محوریت "مخاطره" نسبت به مفاهیم دیگر در ISMS تصریح شده است. در همین راستا به جای "مالک دارایی" از "مالک مخاطره" نام برده شده و طرح برخورد با مخاطرات را منوط به تأیید مالکان مخاطرات کرده تا نشان دهد که استاندارد در نگارش جدید به واقعیت‌های سازمان‌های بزرگ نزدیک‌تر شده است. یکی از مشکلات پیاده‌سازی ISMS در سازمان‌ها این است که در استاندارد قبلی بر مالک دارایی تأکید شده بود در حالی که تهدیدهای امنیتی متوجه مالک مخاطره است نه لزوماً مالک دارایی. در ویرایش قبلی استاندارد، مشخص کردن مالک هر دارایی یک الزام بوده است و همچنین یک ارزیابی آسیب‌پذیری مبتنی بر تهدید پیاده‌سازی می‌شد، که در ویرایش جدید حذف شده و تنها الزام در رابطه با مخاطره، شناسایی آن‌ها با توجه به معیارهای محرمانگی، صحت و دسترس‌پذیری است. در واقع هدف این بوده است که فرایند مدیریت مخاطرات سازگار با استاندارد مدیریت مخاطرات ISO 31000 شود [1,2,3,5].

۷. معیار پذیرش مخاطره[1] می‌تواند چیزی به‌جز سطح مشخصی از مخاطره باشد. به‌عنوان مثال ممکن است سازمان براساس اینکه چه نوع کنترلی برای یک مخاطره مورد نیاز است، آن را قابل پذیرش بداند [۱,۲,۳,۵].

۸. در ویرایش جدید استاندارد بندهای مجزایی در خصوص اهداف، پایش و اندازه‌گیری با قواعد خاص اضافه شده است. این قواعد، الزامی بر تعیین اهداف قابل اندازه‌گیری شفاف دارند و باید مشخص شود که چه شخصی و در چه زمانی آن‌ها را اندازه‌گیری می‌کند و چه شخصی نتایج حاصله را تحلیل و ارزیابی می‌نماید. علاوه‌بر این طرح‌های جامع باید برای تعیین چگونگی حصول اهداف تدوین شوند [1,2,3,7].

۹. تغییر دیگر، حذف اقدامات پیشگیرانه از استاندارد و ادغام با ارزیابی و مدیریت مخاطرات است. علاوه‌بر این بین اقدامات اصلاحی که به‌عنوان یک پاسخ مستقیم به یک عدم انطباق داده می‌شود و اقدامات اصلاحی که برای حذف عامل عدم انطباق استفاده می‌شوند، تمیز قائل شده است [1,2,3,5].

۱۰. در استاندارد جدید بند (۷-۴)، ارتباطات، سازمان باید نیاز به ارتباطات را به همراه مؤلفه‌های چه کسی، با چه کسی، در چه موقعی و به چه منظوری تعیین نماید. از آنجا که هرگونه طرح مرتبط با امنیت اطلاعات با مشارکت همه کارکنان موفقیت‌آمیز خواهد بود و همه کارکنان متولی امنیت در حیطه مسئولیت خود هستند، لذا این بند، مشکل قدیمی که امنیت اطلاعات فقط مربوط به واحد فناوری اطلاعات و یا امنیت است را مرتفع می‌سازد و بر رویکرد نقش‌آفرینی همگان در امنیت تأکید دارد [1,2,3,5].

1. Risk Acceptance Criteria

۳) مدل انتقال از ISO/IEC27001:2005 به ISO/IEC27001:2013

[7,9]

سازمان‌هایی که قبل از این نسبت به استقرار استاندارد ویرایش سال ۲۰۰۵ اقدام کرده‌اند، باید نسبت به اعمال تغییرات ویرایش ۲۰۱۳ استاندارد اقدام نمایند. مدل زیر، گام‌های عملیاتی در این تغییر را بیان می‌کند: [1,2,7,10]

شکل ۴: مدل انتقال از استاندارد ویرایش ۲۰۰۵ به ۲۰۱۳

۱. تهیه فهرست طرف‌های ذینفع

باید تمام طرف‌های ذینفع سازمان شناسایی گردد. ذینفعان افراد و شرکت هایی هستندکه می‌توانند بر امنیت اطلاعات سازمان تاثیر گذارند یا توسط آن تحت تاثیر قرار گیرند مانند سهامداران، سازمان‌های مرتبط و بالادستی، مشتریان، تامین‌کنندگان و شرکای تجاری، خانواده‌های کارکنان، سازمان‌های دولتی، جامعه، رسانه‌ها و...

پس از آن باید فهرستی از تمام الزامات، قراردادها، قوانین، مقررات، انتظارات و غیره فراهم شود. گرچه این موضوع در کنترل‌های استاندارد ویرایش ۲۰۰۵ نیز ذکر شده بود ولی در ویرایش جدید علاوه بر حفظ آن در کنترل الف-۱۸-۱-۱، در بند (۴-۲) متن اصلی استاندارد ذکر شده و از ورودی‌های اصلی برای طرح ریزی ISMS سازمان است .

۲. تعریف تعاملات و رابطها در دامنه کاربرد ISMS

مطابق با ویرایش جدید استاندارد بند (۴-۳)، سازمان باید نسبت به شناسایی تعاملات و رابطها بین فعالیت‌های خود و فعالیت هایی که توسط اشخاص ثالث انجام می شود، اقدام کرده و در بیانیه مدون دامنه کاربرد ذکر نماید.

این تعاملات و رابطها می تواند برای دفاتر سازمانی دیوار و درب باشند و برای سامانه‌های فناوری اطلاعات سازمانی، سوییچ‌ها، دیواره‌های آتش و دستگاه‌های دیگری که آخرین عنصر تحت کنترل سازمان باشد.

۳. همراستایی اهداف ISMS با استراتژی سازمان

مطابق با ویرایش جدید استاندارد بند (۵-۱)، اهداف امنیت تعریف شده باید سازگار با مسیر استراتژیک سازمان باشد. در واقع ویرایش جدید استاندارد به دنبال آن است که نقش ISMS در تحقق اهداف استراتژیک سازمان را شفاف کرده و مشخص کند ISMS چه مزایایی برای کسب‌وکار سازمان به ارمغان خواهد آورد.

برای مثال، اگر شما یک ارائه‌دهنده‌ی خدمات در محیط رایانش ابری بوده و بخشی از استراتژی سازمان، ارائه خدمات قابل اعتمادتر نسبت به رقبا باشد، ISMS سازمان می‌تواند برای رسیدن به این هدف استراتژیک کمک کند چرا که امنیت اطلاعات نه تنها دسترس‌پذیری به نظام را افزایش می‌دهد، بلکه از محرمانگی و یکپارچگی داده نیز محافظت می‌کند .

۴. تغییر خط مشی سطح بالا و کلان امنیت اطلاعات

در ویرایش جدید استاندارد، اصطلاح خط‌مشی ISMS به خط مشی امنیت اطلاعات تغییر کرده است. بر خلاف استاندارد ویرایش ۲۰۰۵، این خط‌مشی می‌تواند شامل الزاماتی مانند همراستایی با مدیریت استراتژیک مخاطرات و معیارهای ارزیابی مخاطره نباشد. همچنین می‌توان در خط مشی امنیت اطلاعات مسئولیت‌های مختلف امنیت اطلاعات را گنجاند. این تغییر بیانگر تغییر رویکرد نگرش به نظام مدیریتی منتج از این استاندارد است. بنظر

می‌رسد استاندارد ویرایش جدید نتیجه گراتر از استاندارد ویرایش ۲۰۰۵ است که در ادامه نیز به شواهد بیشتری از این موضوع اشاره خواهد شد.

۵. ایجاد تغییرات در فرایند ارزیابی مخاطرات

در ویرایش جدید دو تغییر در فرایند ارزیابی مخاطرات وجود دارد: تغییر اول مرتبط با بند (۶-۱-۲-ج-۱) است که دیگر سازمان لازم نیست از روش مبتنی بر شناسایی دارایی‌ها، تهدیدها و آسیب پذیری‌ها استفاده کند به عبارت دیگر سازمان می‌تواند از روش‌های ساده دیگری برای شناسایی مخاطرات استفاده نماید. به عنوان مثال، به جای تعیین جداگانه لپ تاپ به عنوان یک دارایی، ویروس به عنوان یک تهدید و عدم وجود نرم‌افزار ضد ویروس به عنوان یک آسیب پذیری، به سادگی می‌تواند این مخاطره را با عنوان" لپ تاپ می‌تواند توسط یک ویروس مورد حمله قرارگیرد " شناسایی کرد. البته متدلوژی دارایی-تهدید-آسیب‌پذیری کماکان قابل استفاده است.

تغییر دوم مرتبط با بند (۶-۱-۲-ج-۲) است. در ویرایش جدید استاندارد، سازمان باید مالک مخاطره را برای هریک از مخاطرات شناسایی کند. سازمان می‌تواند تصمیم بگیرد که مالکان مخاطره همان مالکان دارایی هستند یا نه. ممکن است سازمان تشخیص دهد که صاحبان مخاطره افرادی هستندکه دارای قدرت کافی برای مدیریت مخاطرات هستند و نه لزوماً مالک دارایی‌ها.

مطلب قابل ذکر دیگر اینکه مطابق بند (۸-۱) ویرایش جدید استاندارد، سازمان باید تمام فرآیندهای برون‌سپاری شده را شناسایی کرده و در مورد چگونگی کنترل آنها تصمیم‌گیری کند. هرچند در استاندارد الزام نشده ولی بهتر است اینکار در طول فرآیند ارزیابی مخاطرات انجام شود. لذا توصیه می‌شود در ارزیابی مخاطرات، خدمات تامین‌کنندگان و شرکا به عنوان یک دارایی گنجانده شده و مخاطرات آنها تعیین شود.

۶. تعیین وضعیت کنترل‌ها در بیانیه کاربست‌پذیری

این مورد یک تغییر کوچک در ویرایش جدید استاندارد است، اما از نقطه نظر پیاده سازی استاندارد قابل توجه است . مطابق بند (۶-۱-۳-د)، در بیانیه کاربست‌پذیری باید برای هر کنترل نشان داده شود که آیا آن کنترل اجرا شده است یا نه. به سادگی می‌توان وضعیت کنترل را دریک ستون جدید قرار داد به عنوان مثال "اجراشده"، "برنامه ریزی شده" و یا "نیمه اجرا شده".

۷. اخذ تاییدیه از مالکان مخاطره

مطابق بند (۶-۱-۳-ج)، باید مالکان مخاطره طرح مقابله با مخاطره و مخاطرات امنیت اطلاعات باقی‌مانده را تایید نمایند. اینکار معمولاً با تایید دو سند مذکور انجام می‌شود. با این حال، اگر مالکان مخاطره متعددی وجود داشته باشد، بهتر است این مسئولیت به مدیریت ارشد واگذار گردد .

۸. طرح‌ریزی ارتباطات نظام‌مند

مطابق بند (۷-۴) ویرایش جدید استاندارد، سازمان باید تعیین کند چه کسی، با چه کسی، در مورد چه موضوعی و چه زمانی ارتباط برقرار خواهد کرد. این مورد در خصوص اشخاص داخلی و خارجی کاربرد دارد. از آنجا که سازمان برای بررسی و تصویب کلیه عناصر ISMS مانند ارزیابی مخاطره، طرح مقابله با مخاطره، کنترل، اندازه گیری، اقدامات اصلاحی، ممیزی داخلی و غیره نیازمند برقراری ارتباط است، لذا بهترین راه برای اینکار، طرح‌ریزی و تعریف ارتباطات مورد نیاز در هر سند و به صورت جداگانه است. به عنوان مثال، در روش ارزیابی مخاطرات و رفع آنها باید تعریف شود که چه کسی از نتایج ارزیابی مخاطرات آگاه شده و با چه کسی در مورد گزینه‌های تعیین شده رفع مخاطره مشورت می‌شود.

۹. تصمیم‌گیری در خصوص رویه‌های مدیریتی مدون ویرایش ۲۰۰۵

در ویرایش جدید استاندارد، الزامی برای انجام اقدامات پیشگیرانه وجود ندارد و در واقع اقدامات پیشگیرانه بعنوان بخشی از فرآیند ارزیابی مخاطرات تلقی شده است، بنابراین سازمان می‌تواند برای حذف یا عدم حذف رویه اقدام پیشگیرانه تصمیم بگیرد.

مطابق بندهای (۷-۵)، (۹-۲) و (۱۰-۱) ویرایش جدید

استاندارد، الزامی به مدون بودن روش‌های اجرایی مرتبط با کنترل مستندات، ممیزی داخلی، و اقدام اصلاحی وجود ندارد، بنابراین می‌توان آنها را نیز حذف کرد، اما باید فرآیندهای آنها حفظ شود حتی اگر روش اجرایی مدون وجود نداشته باشد.

به طور کلی، سازمان‌های کوچکتر تمایل به کاهش تعداد مستندات دارند، در حالی که برای شرکت‌های بزرگ و متوسط یک ایده بهتر مدون کردن روش‌ها و حفظ مستندات است .

۱۰. نوشتن خط‌مشی‌ها و رویه‌های جدید

با انتخاب کنترل‌های مرتبط با بندهای زیر، مطابق ویرایش جدید استاندارد تدوین مستندات مربوطه الزامی است. بنابراین برای حرکت به سمت استقرار استاندارد ویرایش ۲۰۱۳ باید این روش ها در صورت کاربرد، تهیه نمایید:

مطابق با کنترل (الف-۱۴-۱-۵) باید اصول مهندسی نظام امن بصورت مدون ایجاد و پیاده‌سازی شود. این اصول، چگونگی ترکیب و اثرگذاری فنون امنیتی در تمام لایه های معماری شامل معماری کسب و کار، داده، برنامه‌های کاربردی و فناوری را نشان می دهد.

- مطابق با کنترل (الف-۱۵-۱-۱) باید الزامات امنیت اطلاعات برای کاهش مخاطرات مرتبط با تامین کنندگانی که به دارایی‌های سازمان دسترسی دارند، توافق شده و مدون گردد. همچنین این حوزه کنترلی به چگونگی درج بندهای امنیتی در قرارداد، چگونگی پایش تامین‌کنندگان و تغییرات احتمالی مسئولیت‌ها نیز می‌پردازد.
- مطابق با کنترل (الف-۱۶-۱-۵)، رویدادهای امنیتی باید مطابق با یک رویه مدون پاسخ داده شوند. رویه مدیریت حادثه به چگونگی پاسخ به انواع مختلف حوادث، مسئولیت‌ها در این حوزه، افرادی که باید از موضوع مطلع شوند و ... می‌پردازد.
- مطابق با کنترل (الف-۱۷-۱-۲)، فرایندها، رویه‌ها و کنترل‌هایی را برای اطمینان از حفظ سطح مورد نیاز تداوم امنیت اطلاعات در هنگام بحران، ایجاد، مدون و حفظ نماید. رویه‌های تداوم کسب‌وکار، چگونگی بازیابی امنیت کسب‌وکار سازمان و زیرساخت در هنگام بروز یک بحران را بیان می‌کند.

۱۱. سازماندهی مجدد کنترل‌ها

در ویرایش جدید استاندارد، پیوست الف کماکان وجود دارد. حوزه‌های کنترلی از ۱۴ حوزه به ۱۱ حوزه و کنترل‌ها از ۱۳۳ به ۱۱۴ کنترل کاهش یافته‌اند. با این حال، بسیاری از کنترل‌های قدیمی باقی‌مانده‌اند و کنترل‌های جدید عبارتند از:

- الف-۶-۱-۵: امنیت اطلاعات در مدیریت پروژه
- الف-۱۲-۶-۲: محدودیت‌های نصب نرم‌افزار
- الف-۱۴-۲-۱: خط مشی توسعه امن
- الف-۱۴-۲-۵: اصول مهندسی نظام امن
- الف-۱۴-۲-۶: محیط توسعه امن
- الف ۱۴-۲-۸: تست امنیت نظام
- الف-۱۵-۱-۱: خط مشی امنیت اطلاعات برای ارتباط با تامین‌کنندگان
- الف-۱۵-۱-۳: زنجیره تامین فناوری ارتباطات و اطلاعات
- الف-۱۶-۱-۴: ارزیابی و تصمیم گیری در خصوص حوادث امنیت اطلاعات
- الف-۱۶-۱-۵: پاسخ‌دهی به حوادث امنیت اطلاعات
- الف-۱۷-۲-۱: در دسترس بودن امکانات پردازش اطلاعات

۱۲. اندازه‌گیری و گزارش‌دهی

در ویرایش جدید استاندارد، الزامات بسیار صریح‌تر و یا به تعبیری سختگیرانه تر شده‌اند:

- مطابق بند (۶-۲-ب) و به منظور آسان شدن اندازه‌گیری‌ها، اهداف باید حتی المقدور قابل اندازه‌گیری باشند. نمونه‌ای از اهداف امنیت اطلاعات قابل اندازه‌گیری "کاهش تعداد حوادث امنیتی در سال آتی به میزان ۲۵ درصد" است.
- مطابق بندهای (۶-۱-۱-۶-ث) و (۶-۲-د) و به منظور پرداختن به مخاطرات و فرصت‌ها، همه فعالیت‌ها باید ارزیابی شود. بهترین روش برای تحقق این ارزیابی‌ها بهره‌گیری از طرح مقابله با مخاطرات، بیانیه کاربست‌پذیری و همه خط‌مشی‌ها و رویه‌های مدون ISMS است.

• در طرح مقابله با مخاطرات چگونگی پیاده‌سازی کنترل‌ها برای رفع مخاطرات بصورت مدون بیان شده است. برای تحقق ارزیابی همه جانبه مورد نظر ویرایش جدید استاندارد می‌توان در این طرح یک ستون اضافه کرد و چگونگی ارزیابی پیاده‌سازی کنترل را تشریح کرد. در بیانیه کاربست‌پذیری، می‌توان با بیان اهداف در کنار کنترل‌ها و سپس اندازه‌گیری، میزان تحقق و اثربخشی هدف کنترلی را ارزیابی کرد. همچنین در هنگام تدوین هر خط‌مشی و یا رویه باید معیارهایی تحقق اهداف مورد نظر توسط آن ارزیابی خواهد شد، تعیین گردند.

• مطابق بند (۹-۱) ویرایش جدید استاندارد، بصورت شفاف باید مشخص شود چه چیزی، در چه بازه زمانی، توسط چه کسی و چگونه پایش و اندازه‌گیری می‌شود و نتایج را چه کسی ارزیابی می‌کند. علاوه بر این، مطابق بند (۵-۳-ب) باید مسئولیت گزارش‌دهی عملکرد ISMS به وضوح تعیین گردد. بهتر است شرح مسئولیت‌ها در یک سند جداگانه و یا در خط‌مشی‌های امنیت اطلاعات مستند شود. همچنین استفاده از کارت امتیازدهی متوازن و یا مدل‌های مشابه برای پایش و اندازه‌گیری عملکرد ISMS پیشنهاد می شود.

۴) جمع‌بندی و نتیجه گیری

کمیته فنی فناوری اطلاعات JTC۱ با بهره‌گیری از تجارب استقرار این نظام از سال ۲۰۰۵ تا ۲۰۱۳ و با توجه به رویکرد سازمان ISO در سازگارتر کردن استاندارد نظام‌های مدیریتی با یکدیگر و مهم‌تر از همه تغییرات اساسی سال‌های اخیر در حوزه فناوری اطلاعات و امنیت آن، اقدام به انتشار ویرایش جدید این استاندارد کرد. این مقاله در گام نخست به مرور، بررسی و تحلیل تغییرات ویرایش جدید استاندارد نظام مدیریت امنیت اطلاعات،ISO/IEC 27001، پرداخته است.

سپس با توجه به اینکه سازمان‌های دارای گواهینامه انطباق با استاندارد ISO/IEC 27001:2005 ملزم به انتقال به استاندارد ISO/IEC 27001:2013 هستند، مدل عملیاتی برای تسریع در این انتقال ارائه شد. گرچه با بررسی این مقاله و اجرای مدل انتقال، سازمان می‌تواند ادعای انطباق با ویرایش جدید استاندارد را داشته باشد، ولی لازمست دلایل هر گونه تغییری شامل حذف یا اضافه شدن هر بند هرچند کوچک در استاندارد با دید کارشناسی و با نگاه به ماهیت کسب‌وکار و استراتژیک بودن سرمایه‌های اطلاعاتی مورد نظر بررسی گردد تا سازمان در برابر آسیب‌های احتمالی ناشی از عدم بلوغ سازمان در پیاده‌سازی مفاهیم اولیه امنیت و یا تعجیل در حذف فرایندهای مرتبط با بندهای حذف شده در استاندارد بدون توجه به ماهیت آن و ایجاد روش جایگزین و مواردی از این قبیل مصون بماند.

۵) منابع و مراجع

1. ISO/IEC 27001; 2005: Information technology- Security techniques- Information security management systems- Requirements.

2. ISO/IEC 27001:2013: Information technology- Security techniques- Information security management systems- Requirements.

3. ISO/IEC 27002:2013: Information technology- Security techniques- Code of practice for information security controls.

4. An Introduction to ISO/IEC 27001:2013;BSI;2013

5. Overview of ISO/IEC 27001:2013 Wing2i IT solutions; 2013

6. Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013: BSI ; 2013

7. Comparison of Controls between ISO/IEC 27001:2013 & ISO/IEC 27001:2005: Wing2i IT solutions; 2013

8. Twelve-step transition process from ISO 27001:2005 to 2013 revision; Information security and business continuity academy: 2013