INSO-ISO-IEC
27013

1st.Edition

2014

Identical with
ISO/IEC 27013:2012
2014

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ایران-ایزو-آی ای سی

۲۷۰۱۳

چاپ اول

۱۳۹۳

فناوری اطلاعات- فنون امنیتی- راهنمای پیاده‌سازی یکپارچه استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1

Information technology- Security techniques- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ICS: 03.080.99; 35.020; 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود .بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان ملی استاندارد (ISO)[1] ،کمیسیون ملی الکتروتکنیک (IEC)[2] و سازمان ملی اندازه شناسی قانونی (OIML)[3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، به‌منظور پشتیبانی از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به‌منظور حفظ بازارهای ملی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه‌های مدیریت کیفیت و مدیریت زیست-محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه ملی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

---

1 - International Organization for Standardization
2 - International Electrotechnical Commission
3 - International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی - راهنمای پیاده‌سازی یکپارچه استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1»

رئیس:	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق‌لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤول سازمان فنـاوری اطلاعـات ایران
دبیر:	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار)	مدیرکل اداره خدمات ارزش‌افـزوده سـازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
جمیل‌پناه، ناصر (فوق‌لیسانس مدیریت)	کارشناس شرکت مخابرات ایران
سجادیه، علیرضا (فوق‌لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
طی‌نیا، رضا (فوق‌لیسانس مدیریت فناوری اطلاعات)	مدیرعامل شرکت کاربرد سیستم
فولادیان، مجید (فوق‌لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سـازمان فنـاوری اطلاعات ایران
قسمتی، سیمین (فوق‌لیسانس مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سـازمان فنـاوری اطلاعات ایران
مغانی، مهدی (فوق‌لیسانس ریاضی کاربردی)	کارشناس تدوین استاندارد سـازمان فنـاوری اطلاعات ایران
ناظمی، اسلام (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمیدرضا (فوق‌لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی

نیسی مینایی، آصف
(فوق‌لیسانس فناوری اطلاعات)
پژوهش‌گر دانشگاه شهید بهشتی

فهرست مندرجات

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی - راهنمای پیاده‌سازی یکپارچه استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1» که پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و چهل و چهارمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۳/۰۳/۰۳ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد .

منبع و مأخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC 27013:2012, Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

مقدمه

رابطه بین امنیت اطلاعات و مدیریت خدمت به حدی نزدیک است که بسیاری از سازمان‌ها منافع به‌کار گرفتن همزمان هردو استاندارد را تشخیص داده‌اند: استاندارد ISO/IEC 27001، برای امنیت اطلاعات و استاندارد ISO/IEC 20000-1، برای مدیریت خدمت. برای یک سازمان معمول است که شیوه عمل خود را برای مطابقت با الزامات یک استاندارد بین‌المللی بهبود دهد و سپس بهبودهای بیشتری جهت مطابقت با الزامات استاندارد دیگر ایجاد کند.

مزایای بسیاری در پیاده‌سازی یک سامانه مدیریت یکپارچه که نه تنها خدمات فراهم‌شده بلکه محافظت از منابع اطلاعات را به عهده می‌گیرد، وجود دارد. این مزایا می‌توانند در جهت اینکه که آیا یک استاندارد قبل از دیگری یا همزمان پیاده‌سازی شده‌اند، تجربه شوند. فرآیندهای مدیریتی و سازمانی به طور معمول می‌توانند از تشابهات استانداردهای بین‌المللی و اهداف مشترکشان بهره ببرند.

مزایای کلیدی پیاده‌سازی یکپارچه عبارت‌اند از:

الف- اعتبار خدمت کارا و امن برای مشتریان داخلی و خارجی سازمان؛

ب- هزینه کمتر برنامه یکپارچه دو پروژه، درجایی که دستیابی به مدیریت خدمت و امنیت اطلاعات قسمتی از راهبرد سازمان باشد؛

پ- کاهش زمان پیاده‌سازی به علت توسعه یکپارچه فرآیندهایی که در هر دو استاندارد مشترک هستند؛

ت- حذف دوباره‌کاری‌های غیرضروری؛

ث- درک بیشتر مدیریت خدمت و کارمندان امنیت از نقطه‌نظرات یکدیگر؛

ج- سازمانی که برای استاندارد ISO/IEC 27001، تصدیق شده است، آسان‌تر می‌تواند الزامات امنیت اطلاعات در بند ۶-۶ استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱ را برآورده کند، زیرا هر دو استاندارد در الزامات مکمل یکدیگرند.

استاندارد بر اساس نسخه‌های انتشاریافته از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال: ۱۳۸۷[1] و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال: ۱۳۹۱[2]، است.

این استاندارد ملی به‌منظور استفاده توسط اشخاصی با داشتن دانش هردو، داشتن دانش یکی از آن‌ها یا هیچ‌کدام از استانداردهای ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، در نظر گرفته شده است.

انتظار می‌رود همه خوانندگان به نسخه‌هایی از هر دو استاندارد دسترسی داشته باشند. متعاقباً این استاندارد بین‌المللی برخی از قسمت‌های هرکدام از استانداردها را دوباره تولید نمی‌کند. همچنین این استاندارد تمام قسمت‌های هر استاندارد را به طور کامل توصیف نمی‌کند. تنها قسمت‌هایی که در مطلب هم‌پوشانی دارند با جزئیات توصیف شده‌اند.

۱- معادل فارسی استاندارد ISO/IEC 27001:2005

۲- معادل فارسی استاندارد ISO/IEC 20000-1: 2011

این استاندارد بین‌المللی راهنمایی مربوط به قانون و مقررات متنوع خارج از کنترل سازمان، ارائه نمی‌دهد. این قوانین می‌توانند در کشورهای مختلف متفاوت باشد و بر برنامه‌ریزی سامانه مدیریت سازمان تأثیر بگذارد.

فناوری اطلاعات- فنون امنیتی- راهنمای پیاده‌سازی یکپارچه استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی فراهم کردن راهنمایی برای پیاده‌سازی یکپارچه استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، برای سازمان‌هایی است که می‌خواهند:

الف- درحالی‌که استاندارد ISO/IEC 20000-1، پیاده‌سازی شده است، استاندارد ISO/IEC 27001 را نیز پیاده‌سازی کنند یا برعکس؛

ب- استاندارد ISO/IEC 20000-1 و استاندارد ISO/IEC 27001 را با هم پیاده‌سازی کنند؛

پ- سامانه‌های مدیریت استاندارد ISO/IEC 27001 و استاندارد ملی ISO/IEC 20000-1، موجود را با یکدیگر یکپارچه کنند.

این استاندارد بین‌المللی منحصراً بر پیاده‌سازی یکپارچه استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، تمرکز می‌کند.

در عمل استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، می‌توانند با سایر سامانه‌های مدیریتی مانند ISO 9001 و ISO 140001 یکپارچه شوند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، فناوری اطلاعات- مدیریت خدمات - الزامات سامانه مدیریت خدمات.

۲-۲ استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱، فناوری اطلاعات- فنون امنیت - سامانه مدیریت امنیت اطلاعات - مرورکلی و واژگان.

۲-۳ استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، فناوری اطلاعات- فنون امنیتی - سیستم مدیریت امنیت اطلاعات - الزامات.

۳ اصطلاحات، کوته‌نوشت‌ها و تعاریف

در این استاندارد، اصطلاحات و تعاریف استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱، استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱ و اصطلاحات و تعاریف زیر به‌کار می‌رود:

ISMS- سامانه مدیریت امنیت اطلاعات[1] (از استاندارد ISO/IEC 27001)

SMS- سامانه مدیریت خدمت[2] (از استاندارد ISO/IEC 20000-1)

پیوست الف از این استاندارد ملی مقایسه‌ای در سطح بند از محتوای بین استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱ و استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، ارائه کرده است.

پیوست ب در این استاندارد بین‌المللی مقایسه‌ای از اصطلاحاتی که در موارد زیر تعریف‌شده است، ارائه می‌دهد:

- استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱، واژگان برای استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷؛
- اصطلاحاتی که در استاندارد ISO/IEC 27001، به‌کار می‌روند؛
- اصلاحاتی که در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، تعریف یا استفاده شده‌اند.

۴ مرور کلی بر استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1

۴-۱ شناخت استاندارد بین‌المللی

توصیه می‌شود یک سازمان قبل از برنامه‌ریزی برای سامانه مدیریت یکپارچه درک مناسبی از ویژگی‌ها، شباهت‌ها و تفاوت‌های استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، داشته باشد. این درک، زمان و منابع در دسترس برای پیاده‌سازی را بیشینه می‌سازد. بند ۴-۲ تا ۴-۴ از این استاندارد ملی مقدمه‌ای بر مفاهیم عمده اساسی هر دو استاندارد ارائه می‌دهد، اما توصیه نمی‌شود به‌عنوان جایگزین بازنگری با جزئیات به‌کار رود.

۴-۲ مفاهیم استاندارد ISO/IEC 27001

استاندارد ISO/IEC 27001، نمونه‌ای برای برقراری، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود ISMS برای محافظت از دارایی‌های اطلاعاتی فراهم می‌کند. دارایی اطلاعاتی، شامل اطلاعات در هر شکل، ذخیره‌شده در هر نوع و مورد استفاده برای هرگونه هدف توسط سازمان یا درون سازمان می‌شود.

برای مطابقت با استاندارد ISO/IEC 27001، توصیه می‌شود سازمان ISMS را بر اساس فرآیند ارزیابی مخاطره، برای شناسایی مخاطرات دارایی‌های اطلاعاتی، پیاده‌سازی کند. به‌عنوان قسمتی از این کار، توصیه می‌شود سازمان سنجه‌های متنوعی را برای مدیریت این مخاطرات انتخاب، پیاده‌سازی، پایش و بازنگری کند. این سنجه‌ها تحت عنوان کنترل‌ها شناخته می‌شوند. سازمان بهتر است سطح قابل‌قبولی از مخاطره را

1- Information Security Management System (ISMS)

2- Service Management System (SMS)

با در نظر گرفتن الزامات کسب‌وکار و الزامات تحمیل‌شده خارجی، مشخص کند. نمونه‌ای از الزامات تحمیل‌شده خارجی، الزامات قوانین مدون و تنظیم‌شده و تعهدات قراردادی می‌باشند.
سازمان با هر اندازه و نوعی می‌تواند استاندارد ISO/IEC 27001 را به‌کار ببرد.

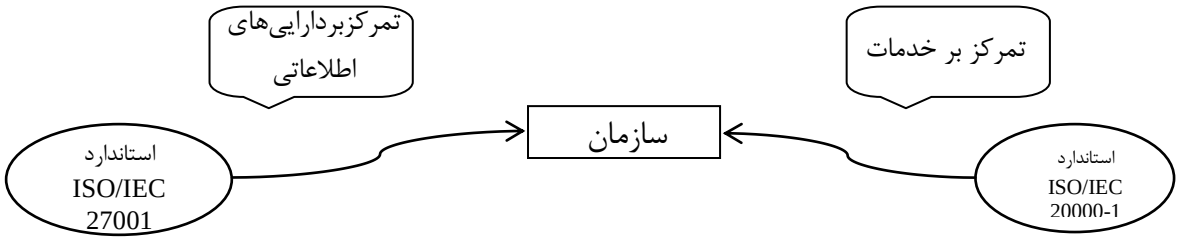
۳-۴ مفاهیم استاندارد ISO/IEC 20000-1

استاندارد ISO/IEC 20000-1، می‌تواند توسط سازمان‌ها، یا قسمت‌هایی از سازمان‌ها که از خدمات استفاده می‌کنند یا آن را ارائه می‌دهند، استفاده شود. این کار برای مشتری و ارائه‌دهنده خدمت ارزش ایجاد می‌کند. هرچند، همه فرآیندهایی که توسط استاندارد پوشش داده می‌شوند توسط فراهم‌کننده خدمت کنترل می‌شوند و این تنها فراهم‌کننده خدمت است که می‌تواند به انطباق با استاندارد ISO/IEC 20000-1، دست یابد. استاندارد اساساً برای اطمینان از این است که خدمات، الزامات خدمت را برآورده کنند و برای مشتری و فراهم‌کننده خدمت ایجاد ارزش کنند.
مدیریت خدمت، فعالیت‌ها و منابع یک فراهم‌کننده خدمت را در طراحی، توسعه، انتقال، تحویل و بهبود خدمات، برای برآوردن الزامات خدمت، همان‌طورکه با مشتری توافق کرده‌اند، هدایت و کنترل می‌کند.
برای برآوردن الزامات استاندارد، طیفی از فرآیندهای مدیریت خدمت خاص بهتر است توسط فراهم‌کننده خدمت پیاده‌سازی شود. این فرآیندهای خاص در بین سایر فرآیندها شامل مدیریت رخداد، مدیریت تغییر و مدیریت مشکل است. مدیریت امنیت اطلاعات یکی از فرآیندهای مدیریت خدمت استاندارد ISO/IEC 20000-1، است.
سازمان با هر اندازه و نوعی می‌تواند استاندارد ISO/IEC 20000-1 را به‌کار ببرد.

۴-۴ تشابهات و تفاوت‌ها

مدیریت خدمت و مدیریت امنیت اطلاعات به طور معمول به گونه‌ای تلقی می‌شوند که نه متصل[1] و نه وابسته[2] هستند. مفهوم این جداسازی این است که مدیریت خدمت می‌تواند به سادگی به‌کارایی و سودآوری مربوط شود، درحالی‌که مدیریت امنیت اطلاعات اغلب به‌عنوان پایه‌ای برای تحویل خدمت مؤثر درک نمی‌شود. در نتیجه، مدیریت خدمت اغلب در ابتدا پیاده‌سازی می‌شود. هرچند همان طور که در شکل ۱ نشان داده شده است، بسیاری از اهداف کنترلی و کنترل‌ها در پیوست الف از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، شامل الزامات مدیریت خدمت در استاندارد ISO/IEC 20000-1 نیز می‌شود.

1- Connected
2- Interdependent



مختص ISO/IEC 20000-1	قسمت‌های به اشتراک گذاشته‌شده (برخی همپوشانی، برخی تفاوت‌ها)		مختص ISO/IEC27001
- بودجه‌بندی و حسابداری خدمت - مدیریت روابط کسب‌وکار - طراحی و انتقال خدمات جدید یا تغییریافته - مدیریت سطح خدمت	- مدیریت منابع - ارزیابی مخاطره - نقش‌ها و مسئولیت‌ها - مدیریت امنیت اطلاعات - مدیریت تداوم خدمت و قابلیت دسترسی - مدیریت تأمین‌کننده	- مدیریت ظرفیت - مدیریت تغییر - مدیریت پیکربندی - مدیریت رخداد و درخواست خدمت - مدیریت مشکل - مدیریت انتشار و استقرار	- طبقه‌بندی اطلاعات - مدیریت منابع اطلاعاتی
قسمت مشترک (یکسان بین هر دو استاندارد)			
- بهبود مستمر - انطباق قانونی و مقرراتی - بازنگری مدیریتی		- PDCA - آموزش و آگاه‌سازی - مدیریت مستندسازی	

شکل ۱- مقایسه مفاهیم در استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1،

مدیریت امنیت اطلاعات و مدیریت خدمت به وضوح فرآیندها و فعالیت‌های بسیار مشابهی دارند، ولو اینکه یکی از سامانه‌های مدیریتی برخی جزئیات را بیشتر از دیگری برجسته کرده باشند. برای اطلاعات بیشتر به پیوست الف از این استاندارد بین‌المللی مراجعه کنید. وقتی با دو استاندارد کار می‌کنیم بهتر است درک شود که آن‌ها در بیش از یک جهت دارای ویژگی های متفاوت هستند. برای مثال محدوده آن‌ها متفاوت است، به بند ۵-۲ از این استاندارد بین‌المللی مراجعه شود. آن‌ها اهداف متفاوتی دارند. استاندارد ISO/IEC 20000-1، طراحی شده است تا اطمینان دهد که سازمان خدمات مؤثری ارائه می‌کند، درحالی‌که استاندارد ISO/IEC 27001، طراحی شده است تا سازمان را برای مدیریت مخاطره امنیت اطلاعات و پیشگیری از رخدادهای امنیتی توانمند سازد.

۵ رویکردهای پیاده‌سازی یکپارچه

۵-۱ کلیات

سازمانی که در حال طرح‌ریزی برای پیاده‌سازی استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، است، می‌تواند یکی از سه حالت زیر را داشته باشد:

- چیدمان‌های مدیریت اقتضایی موجود اند به طوری‌که امنیت اطلاعات و مدیریت خدمت را پوشش می‌دهند (همچنین سامانه‌های مدیریت رسمی در حوزه‌های دیگر می‌توانند وجود داشته باشند، مانند مدیریت کیفیت).
- سامانه مدیریتی بر اساس یک استاندارد وجود دارد.
- سامانه‌های مدیریت بر اساس دو استاندارد وجود دارند، اما یکپارچه نیستند.

توصیه می‌شود سازمانی که در حال طرح‌ریزی برای پیاده‌سازی سامانه مدیریت یکپارچه است حداقل موارد زیر را در نظر داشته باشد:

الف- سایر سامانه (های) مدیریتی که در حال استفاده هستند (مانند سامانه مدیریت کیفیت)؛

ب- همه خدمات، فرآیندها و وابستگی آنها در مفهوم سامانه مدیریت یکپارچه؛

پ- عناصر هر استاندارد که می‌توانند ادغام شوند و چگونگی ادغام آنها؛

ت- عناصری که باید جدا بمانند؛

ث- تأثیر سامانه مدیریت یکپارچه بر روی مشتری‌ها، تأمین‌کنندگان و سایر طرف‌ها؛

ج- تأثیر بر فناوری در حال استفاده؛

چ- تأثیر یا مخاطره بر خدمات و مدیریت خدمت؛

ح- تأثیر یا مخاطره بر امنیت اطلاعات و مدیریت امنیت اطلاعات؛

خ- تحصیلات و آموزش در سامانه مدیریت یکپارچه؛

د- گام‌ها و توالی فعالیت‌های پیاده‌سازی.

۲-۵ ملاحظات دامنه کاربرد

یکی از نواحی که دو استاندارد بین‌المللی به طور قابل‌ملاحظه‌ای در آن متفاوت هستند، موضوع محدوده کاربرد است، بدین معنا که سامانه مدیریت بهتر است دارایی‌ها، فرآیندها و قسمت‌های سازمان را شامل شود. استاندارد ISO/IEC 20000-1، در رابطه با الزامات برای طراحی، انتقال، تحویل و بهبود خدمات برای برآوردن الزامات است. این هدف از طریق مجموعه‌ای از فرآیندها حاصل می‌شود. از این رو محدوده استاندارد ISO/IEC 20000-1، شامل فرآیندهای مدیریتی درون سازمان و خدمات، فراهم شده است. استاندارد ISO/IEC 27001، در رابطه با چگونگی مدیریت مخاطره امنیت اطلاعات است. محدوده استاندارد ISO/IEC 27001، قسمت‌هایی از فعالیت‌هایش را که سازمان تمایل دارد امن باشد، پوشش می‌دهد. به این معنا، محدوده هر دو استاندارد متفاوت معنا می‌شوند. در نتیجه پیاده‌سازی استاندارد ISO/IEC 27001، برای محدوده مشابه استاندارد ISO/IEC 20000-1، ممکن است، اما استاندارد ISO/IEC 20000-1، نمی‌تواند بر کل سازمان اعمال شود مگر اینکه سازمان کاملاً فراهم‌کننده خدمت باشد.

بنابراین فرآیندها، دارایی‌ها و نقش‌های مشخصی باید از محدوده مستثنا شوند تا یک ISMS توسعه‌یافته، با استاندارد ISO/IEC 27001، مطابقت یابد. برای استاندارد ISO/IEC 20000-1، اگر این فرآیندها، دارایی‌ها و نقش‌ها قسمتی از محدوده SMS یا همکار در محدوده SMS باشند، ممکن است از محدوده مستثنا نشوند.

همچنین محدوده ISMS ممکن است منحصراً با محدوده فیزیکی مشخص، مانند فضای احاطه‌کننده امنیتی، تعریف شوند.

در برخی موارد دو استاندارد بین‌المللی نمی‌توانند برای همه یا حتی قسمتی از فعالیت‌های سازمان پیاده‌سازی شوند. برای مثال سازمانی که به علت نداشتن حاکمیت بر همه فرآیندهایی که توسط طرف‌های دیگر انجام می‌شود، نمی‌تواند با الزامات استاندارد ISO/IEC 20000-1، انطباق یابد.

یک سازمان می‌تواند یک SMS و یک ISMS با برخی همپوشانی‌ها بین حوزه‌های کاربردی مختلف پیاده‌سازی کند. جایی که فعالیت‌ها بین محدوده استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، قرارگرفته‌اند، توصیه می‌شود سامانه مدیریت یکپارچه هردو استاندارد را در نظر بگیرد، به پیوست الف از این استاندارد بین‌المللی مراجعه کنید. تفاوت‌ها در محدوده می‌تواند باعث شود برخی خدمات که در SMS وجود دارند در ISMS مستثنا شوند. به همان اندازه SMS می‌تواند فرآیندها و کارکردهای ISMS را مستثنا کند. برای مثال برخی از سازمان‌ها تصمیم می‌گیرند یک ISMS را تنها در توابع عملیاتی و ارتباطی خود پیاده‌سازی کنند، درحالی‌که SMS آنها خدمات مدیریت کاربرد را شامل می‌شود. متناوباً ISMS می‌تواند همه خدمات را پوشش دهد، درحالی‌که SMS تنها خدمات برای مشتریان ویژه یا برخی خدمات برای همه مشتریان را پوشش می‌دهد. توصیه‌می‌شود سازمان حوزه‌های کاربرد استانداردها را تا حد امکان تنظیم کند تا اطمینان حاصل شود که سامانه مدیریت می‌تواند با موفقیت یکپارچه شود.

یادآوری- راهنما برای تعریف محدوده برای استاندارد ISO/IEC 20000-1، در ISO/IEC 20000-3:2012، راهنمایی در تعریف محدوده و کاربست‌پذیری ISO/IEC 20000-1، در دسترس است.

۵-۳ فرانامه‌های پیش از پیاده‌سازی

۵-۳-۱ کلیات

همان طور که در بند ۵-۳-۲ تا ۵-۳-۴ این استاندارد بین‌المللی توصیف شده است، سازمانی که یک سامانه مدیریت یکپارچه طرح‌ریزی می‌کند، می‌تواند در یکی از سه حالت باشد. در تمام موارد، سازمان دارای گونه‌ای از فرآیندهای مدیریتی است، درغیراین‌صورت وجود نخواهد داشت. بندهای زیر پیشنهادهایی برای پیاده‌سازی در هر سه حالت که دربند ۵-۲ این استاندارد نیز توضیح داده‌شده‌اند، ارائه شده است.

۵-۳-۲ هیچ استانداردی در حال حاضر به‌عنوان مبنای سامانه مدیریت به‌کار نمی‌رود

تصور جایی که هیچ‌کدام از استانداردها پیاده‌سازی نشده باشد راحت است، هیچ خط مشی، فرآیند و روالی وجود ندارد، بنابراین رسیدگی کردن به وضعیت ساده است. متأسفانه این یک تصور غلط است. سازمانی که سامانه مدیریتی بر اساس استاندارد ISO/IEC 27001، یا استاندارد ISO/IEC 20000-1، ندارد احتمالاً دارای شکلی از سامانه مدیریت است. این سامانه باید تعدیل شده تا به انطباق با یکی یا هر دو استاندارد برسد.

تصمیم مربوط به ترتیب پیاده‌سازی دو سامانه مدیریت، بهتر است بر اساس نیازهای کسب‌وکار اتخاذ شود. تصمیم می‌تواند بر اساس اینکه آیا انگیزه، ایجاد موقعیت رقابتی با استفاده از یک استاندارد یا دیگری است یا یک نیاز برای نشان دادن الزامات یک استاندارد یا دیگری برای مشتری موجود یا جدید وجود دارد، تحت تأثیر قرار می‌گیرد.

یک تصمیم مهم دیگر این است که آیا پیاده‌سازی یک سامانه مدیریت از ابتدا بر اساس هر دو استاندارد، یا پیاده‌سازی یک سامانه مدیریت بر اساس یک استاندارد صورت گیرد و سپس جهت در برگرفتن الزامات دیگری توسعه داده شود، به بند ۵-۳-۳ از این استاندارد بین‌المللی مراجعه کنید. هر دو استاندارد می‌توانند به طور همزمان پیاده‌سازی شوند، اگر فعالیت‌ها و تلاش‌های پیاده‌سازی بتوانند هماهنگ شوند و تکرار حداقل شود. هرچند بر اساس ماهیت سازمان احتیاط بر این است که با یک استاندارد آغاز شود و سپس دیگری پیاده‌سازی شود.

این ملاحظات در فرانامه‌های زیر توصیف شده‌اند:

الف- توصیه می‌شود سازمانی که خدماتی فراهم می‌کند با پیاده‌سازی استاندارد ISO/IEC 20000-1، آغاز کند و با به‌کارگیریبه‌کار درس‌های آموخته‌شده در طول پیاده‌سازی، سامانه مدیریت را توسعه دهد تا شامل استاندارد ISO/IEC 27001 نیز شود.

ب- سازمانی که از تأمین‌کنندگان استفاده می‌کند و شامل سایر طرف‌هاست، بهتر است برای تحویل برخی از اجزای خدمات، ابتدا بر استاندارد ISO/IEC 20000-1، تمرکز کند. این اقدام الزامات بیشتری را شامل مدیریت تأمین‌کننده برای طرف‌ها فراهم می‌کند. این عمل تفکیک مدیریت تأمین‌کننده و موضوعات کنترل فرآیند را ممکن می‌کند. توصیه می‌شود سپس سازمان به سمت استاندارد ISO/IEC 27001، حرکت کند.

پ- سازمان‌های کوچک بهتر است بر اساس سطح وابستگی خود به مدیریت خدمت یا امنیت اطلاعات بر استاندارد ISO/IEC 27001، یا استاندارد ISO/IEC 20000-1، تمرکز کنند.

ت- سازمان‌های بزرگ با تحویل خدمت داخلی، بهتر است پیاده‌سازی را به‌عنوان یک پروژه ساده ساماندهی کنند. اگر این کار ممکن نباشد، سپس توصیه می‌شود سازمان پیاده‌سازی را به دو زیر پروژه با یک برنامه فراگیر کاری تقسیم کند. توصیه می‌شود هر زیر پروژه باید یک استاندارد را مدیریت، و به‌عنوان یک زیر پروژه در ادامه پیاده‌سازی را یکپارچه کند. اگر این رویکرد انتخاب شود، اطمینان از اینکه پیاده‌سازی‌های در حال توسعه سازگار هستند، حیاتی است. این رویکرد می‌تواند سربار اضافه و مخاطره مازاد بر خروجی وارد کند، بنابراین توصیه می‌شود تنها وقتی به‌کار رود که هیچ جایگزینی وجود نداشته باشد.

ث- در هر سازمانی که امنیت اطلاعات دارای سطح بالایی از اهمیت است، بهتر است در ابتدا ISMS پیاده‌سازی شود که با الزامات استاندارد ISO/IEC 27001، مطابقت داشته باشد. توصیه می‌شود برای پشتیبانی امنیت اطلاعات مرحله بعد توسعه آن سامانه مدیریت است تا الزامات استاندارد ISO/IEC 20000-1، برآورده کند.

یک گروه کاری یکپارچه و جلسات منظم در طول پیاده‌سازی هر دو استاندارد کمک می‌کند اطمینان حاصل شود که هر دو استاندارد با یکدیگر هم‌تراز هستند.

۵-۳-۳ یک سامانه مدیریت وجود دارد که الزامات یکی از استانداردها را برآورده می‌کند

در جایی که از قبل یک سامانه مدیریت با یکی از دو استاندارد مطابقت دارد، توصیه می‌شود هدف اصلی یکپارچه‌سازی الزامات با استاندارد دیگر باشد. این هدف بهتر است بدون تحمیل هرگونه خسارت یا به خطر

انداختن امنیت اطلاعات یک خدمت انجام شود. به‌هرحال توصیه می‌شود سامانه مدیریت موجود بـه عناصـر منفردش شکسته شود. این امر بهتر است به‌دقت از پیش برنامـه‌ریـزی و بـا مسـتندات موجـود کـه توسـط خبرگان در استاندارد معرفی‌شده‌اند، بازنگری شود و توسط آن‌ها در استاندارد حاضر، پیاده‌سازی شود.
توصیه می‌شود سازمان ویژگی‌های سامانه مدیریت برقرارشده را شناسایی کند که حداقل موارد زیر را شامل شود:

الف- محدوده کاربرد؛
ب- ساختار سازمانی؛
پ- خط مشی‌ها؛
ت- اقدامات طرح‌ریزی؛
ث- مجوزها و مسئولیت‌ها؛
ج- رویه‌ها؛
چ- روشگان‌های مدیریت مخاطره؛
ح- فرآیندها؛
خ- روال‌ها؛
د- اصطلاحات و تعاریف؛
ذ- منابع.

سپس توصیه می‌شود این ویژگی‌ها بازنگری شوند تا مشخص شود چگونـه مـی‌تواننـد بـه سـامانه مـدیریت یکپارچه اعمال شوند. اگر رویکرد دو مرحله‌ای با یک سامانه مدیریت کار گذاشته‌شده، به‌عنـوان مرحلـه اول استفاده می‌شود، گام دوم پیاده‌سازی سامانه مدیریت دیگر است. توصیه می‌شود محدوده کاربرد هـر مرحلـه قبل از شروع هرگونه کار پیاده‌سازی مشخص و توافق شود.

۵-۳-۴ سامانه‌های مدیریت جداگانه‌ای وجود دارند که الزامات هرکدام از استانداردها را برآورده مـی-کنند.

این مورد آخر، شاید پیچیده‌ترین مورد باشد. این مورد موضوع محدوده کاربرد را شرح می‌دهد، به بنـد ۵-۲ از این استاندارد بین‌المللی مراجعه کنید. ممکن است یک سـازمان، اسـتاندارد ISO/IEC 27001 را در یـک ناحیه و استاندارد ISO/IEC 20000-1 را در ناحیه دیگری از سازمان پیاده‌سازی کرده باشد. سپس سـازمان می‌تواند تصمیم بگیرد یکی از استانداردها را با حیطه وسیع‌تری از فعالیت‌ها اعمال کند. در بسیاری از نقـاط زمان، سامانه‌های مدیریتی برای فعالیت‌های مشابهی پیاده‌سازی می‌شوند. به طور متناوب دو سـازمان مـی-توانند برای ادغام شدن برنامه‌ریزی کنند. یکی مطابقت با استاندارد ISO/IEC 27001 و دیگری مطابقـت بـا استاندارد ISO/IEC 20000-1 را نشان می‌دهند.
توصیه می‌شود بازنگری نقطه آغاز را با هدف دستیابی به موارد زیر شکل دهد:

الف- شناسایی و مستند کردن حوزه‌های کاربردی موجود و پیشنهادشده هر استاندارد، بـا توجـه ویـژه بـه تفاوت‌های آن‌ها.
ب- مقایسه سامانه‌های مدیریت موجود و در صورت وجود، تعیین نمودن ابعاد ناسازگاری دوجانبه.

پ- آغاز به درگیرکردن ذینفعان در هر دو سامانه مدیریت با یکدیگر.

ت- برنامه‌ریزی بهترین رویکرد به سمت یک سامانه مدیریت یکپارچه:

۱- شروع با رئوس مطالب بسیار گسترده.

۲- بازنگری آن در سطوح مختلف در سازمان برای اضافه کردن جزئیات.

۳- ارائه بازخورد و راه‌حل‌های پیشنهادشده به سطح مناسبی از اختیار تا گرفتن تصمیم‌گیری تصویب شود.

هرچند راه‌های متعددی برای یکپارچه‌سازی سامانه‌های مدیریتی با حفظ انطباق وجود دارد، اما بهتر است یک گام برنامه‌ریزی گسترده کامل شود.

۶ ملاحظات پیاده‌سازی یکپارچه

۶-۱ کلیات

توصیه می‌شود در همه موارد هدف سازمان تولید یک سامانه مدیریت یکپارچه بادوام باشد که مطابقت با هردو استاندارد را امکان‌پذیر سازد. هدف، مقایسه استانداردها یا مشخص کردن اینکه کدام یک بهتر یا درست است، نیست. جایی که تعارض بین نقطه‌نظرات وجود دارد، بهتر است به گونه‌ای حل شود که الزامات هر دو استاندارد را برآورده کند و اطمینان دهد که سازمان به بهبود مستمر در ISMS و SMS دست می‌یابد. توصیه می‌شود سامانه مدیریت یکپارچه ایده‌آل بر اساس کاراترین رویکردها از هر دو استاندارد باشد و به طور مناسب اعمال شود. همچنین این رویکرد با کاربرد جزئیات بیشتر در یک استاندارد برای تکمیل دیگری، پشتیبانی می‌شود. توصیه می‌شود به هر آنچه برای مطابقت با هردو استاندارد مورد نیاز است، توجه شود.

قابلیت ردگیری مستند بهتر است بین سامانه مدیریت یکپارچه و الزامات هر استاندارد جداگانه اعمال شود. جهت کاهش تلاش، یک مجموعه واحد از مستندات می‌تواند برای سامانه مدیریت یکپارچه ایجاد شود. برای پشتیبانی از آن یک سازمان می‌تواند مستند قابل ردگیری مانند ماتریس ردیابی ایجاد کند. این ماتریس به وضوح نشان می‌دهد که چگونه سامانه مدیریت یکپارچه با الزامات هرکدام از استانداردها مطابقت می‌کند. مزیت این رویکرد شامل توانمند بودن برای نشان دادن راحت مطابقت در ممیزی‌ها و بازنگری می‌شود. همچنین این مزایا، شامل قابلیت ردگیری فعالیت‌های ضروری برای نشان دادن مطابقت با هر استاندارد است.

۶-۲ چالش‌های بالقوه

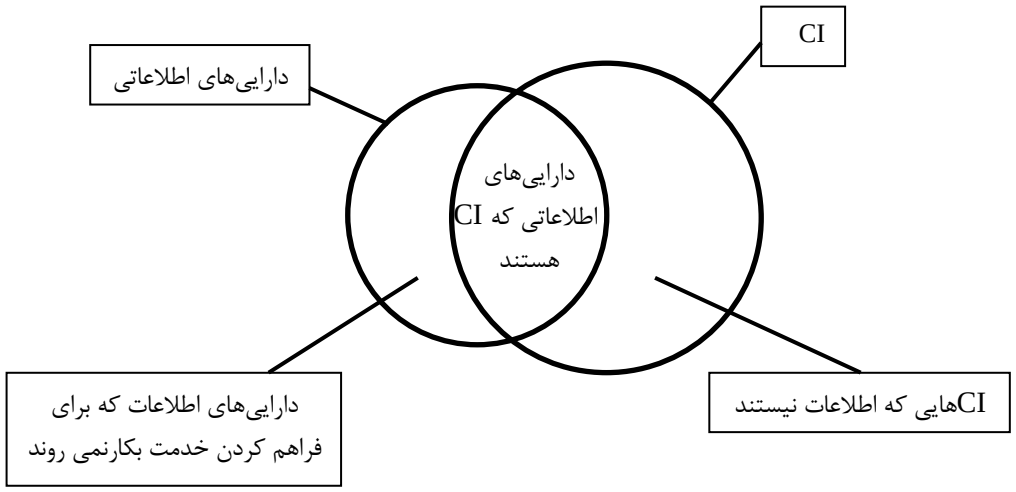
۶-۲-۱ کاربرد و منظور دارایی

دارایی در استاندارد ISO/IEC 20000-1، با دارایی اطلاعاتی در استاندارد ISO/IEC 27001، متفاوت است. دارایی یک اصطلاح تعریف‌شده در استاندارد ISO/IEC 20000-1، نیست، بنابراین در معنای انگلیسی معمول به معنای یک چیز باارزش به‌کار می‌رود. در برخی از بندهای استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، کاربرد دارایی‌ها، به دارایی‌های مالی مانند مجوزهای نرم‌افزاری ارتباط داده شده است. در سایر بندها به دارایی‌ها به‌عنوان دارایی‌های اطلاعاتی ارجاع داده شده است. در مقابل استاندارد

ISO/IEC 27001، بر اساس مفهوم محافظت از اطلاعات بناشده است و یک تعریف رسمی از دارایی اطلاعاتی دارد. در مابقی بند ۶,۲ از این استاندارد بین‌المللی، تفاوت‌ها و شباهت‌های کاربرد و معنی در هر دو استاندارد بحث می‌شود. پیشنهادهایی از چگونگی مطابقت هر دو استاندارد را شامل می‌شود.

استاندارد ISO/IEC 20000-1، از یک اصطلاح تعریف‌شده استفاده می‌کند، مورد پیکربندی (CI)[1]، به‌عنوان عنصری که جهت تحویل خدمت یا خدمات نیاز به کنترل شدن دارد. بنابراین توصیه می‌شود سازمان با در نظر گرفتن نیاز خود به کارایی، CI اهداف خود را مشخص کند. «دارایی اطلاعاتی» می‌تواند در این تعریف شامل شود. در استاندارد ISO/IEC 20000-1، دادگان مدیریت پیکربندی، انبار داده همه CIها و روابط آنهاست. برخی دارایی‌های سازمانی در دادگان مدیریت پیکربندی نخواهند بود (برای مثال رایانه‌های شخصی که برای تحویل خدمت به‌کار نمی‌روند). به همان ترتیب برخی از CIها مانند افراد، ممکن است تحت استاندارد ISO/IEC 20000-1، به‌عنوان دارایی در نظر گرفته نشوند. دارایی در استاندارد ISO/IEC 20000-1، به طور معمول دارای ارزش پولی است.

در استاندارد ISO/IEC 27001، دارایی‌های اطلاعاتی به‌عنوان دانش یا داده‌ای که بدون توجه به نوعشان برای سازمان دارای ارزش هستند، تعریف‌شده است؛ مانند کاغذ، الکتریسیته، ... در نتیجه دارایی‌های اطلاعاتی می‌توانند CI باشند اما CIها لزوماً دارایی اطلاعاتی نیستند. برای مثال یک کابل داده[2] می‌تواند یک CI باشد، اما معمولاً یک دارایی اطلاعاتی نیست. شکل ۲ توصیفی از ارتباط بین CIها و دارایی‌های اطلاعاتی ارائه می‌دهد. برای یک سامانه مدیریت یکپارچه، یک دارایی اطلاعاتی در استاندارد ISO/IEC 27001، می‌تواند توسط یک خدمت در استاندارد ISO/IEC 20000-1، استفاده شود یا قسمتی از یک خدمت باشد.



شکل ۲- ارتباط بین دارایی‌های اطلاعاتی در استاندارد ISO/IEC 27001 و CIها در استاندارد ISO/IEC 20000-1

1- Configuration Item
2- Data cable

هیچ‌کدام از استانداردها الزامی به اینکه هر CI یا دارایی اطلاعاتی به طور مجزا فهرست شود ندارند. آنها می‌توانند در انواعی مانند سخت‌افزار یا مستندات گروه‌بندی شوند. به‌عنوان قسمتی از این فرآیند، توصیف آنها بهتر است تا حد امکان سازگار باشد تا انطباق با هر دو استاندارد را ساده کند. برای مثال در ابتدای هرگونه یکپارچه‌سازی، توصیه می‌شود تصمیمی در رابطه با راهی که در آن دارایی‌ها دسته‌بندی یا شناسایی می‌شوند، اتخاذ شود. این کار جهت حصول اطمینان از این است که بتوان منابع غیرمبهمی به دارایی‌ها ارجاع داد. اگر اصطلاح دارایی اطلاعات در استاندارد ISO/IEC 27001، به‌کار رود، بهتر است به دارایی‌های خاص برچسب مازاد زده شود تا اطمینان حاصل شود که وضعیتشان به‌عنوان CIها یا دارایی‌های مالی در استاندارد ISO/IEC 20000-1، شناخته‌شده است، به پیوست ب از این استاندارد بین‌المللی مراجعه کنید.

۶-۲-۲ طراحی و انتقال خدمت

بند ۵ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل الزاماتی برای طراحی و انتقال خدمات جدید یا تغییریافته است. بند معادل مستقیمی در استاندارد ISO/IEC 27001، وجود ندارد، اگرچه ابعاد مختلفی از طراحی، انتقال و تحویل در پیوست الف از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، پوشش داده شده است. هرچند یک سامانه مدیریت یکپارچه باید تضمین کند که امنیت اطلاعات با جزئیات، در طول گام‌های برنامه‌ریزی طراحی و انتقال خدمات جدید یا تغییریافته در نظر گرفته شده است. موضوعاتی که بهتر است در نظر گرفته شود شامل یک ارزیابی از تأثیر خدمت جدید یا تغییریافته بر خدمت و کنترل‌های امنیت اطلاعات موجود است، به بند ۶-۲-۲ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مراجعه کنید. توصیه می‌شود این ارزیابی همچنین برای خاتمه خدمت انجام شود.

توصیه می‌شود برنامه‌ریزی همه خدمات جدید یا تغییریافته دربرگیرنده ملاحظات امنیت اطلاعات باشد. این عمل بهتر است صرف‌نظر از اینکه آیا خدمت در محدوده ISMS قرار می‌گیرد یا خیر انجام پذیرد.

۶-۲-۳ مدیریت و ارزیابی مخاطرات

بندهای ۴-۵-۲ و ۴-۵-۳ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل الزامات ارزیابی مخاطره و همچنین برطرف‌سازی مخاطرات مرتبط با SMS است.

بند ۴-۲-۱ از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، الزامات برای مدیریت همه جنبه‌های مرتبط با امنیت اطلاعات را ارائه می‌دهد. الزامات محدود به مخاطرات مرتبط با ISMS نمی‌شوند و ارزیابی و برطرف‌سازی مخاطرات و سایر جنبه‌های مدیریت مخاطره امنیت اطلاعات را در بر می‌گیرند.

اگرچه مخاطرات در هر دو استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، در نظر گرفته شده است، ماهیت این مخاطرات متفاوت است. استاندارد ISO/IEC 20000-1، مخاطرات سامانه امنیت اطلاعات و خدمات را در برمی‌گیرد، درحالی‌که استاندارد ISO/IEC 27001، مخاطره امنیت اطلاعات و چگونگی تأثیرش بر سازمان را در نظر می‌گیرد. معیارهای ارزشیابی و برطرف کردن مخاطرات بر اساس اینکه آیا مخاطرات در ارتباط با تحویل یک خدمت یا به طور مشخص برای امنیت اطلاعات هستند، متفاوت است. هرچند روشی که برای شناسایی مخاطرات به‌کار می‌رود می‌تواند در هر دو استاندارد یکسان باشد. برخی مخاطرات که توسط استاندارد ISO/IEC 20000-1، در نظر گرفته می‌شوند، برای مثال مخاطره تأمین‌کننده که به هزینه‌های مربوط به توافقنامه سطح خدمت بی‌توجه است، از نقطه‌نظر استاندارد ISO/IEC 27001،

مخاطره در نظر گرفته نمی‌شود؛ بنابراین مخاطرات شناسایی‌شده با استفاده استاندارد ISO/IEC 20000-1، نمی‌توانند مربوط به امنیت اطلاعات فرض شوند و برعکس.

همچنین مالکیت مخاطره بین دو رویکرد می‌تواند متفاوت باشد. برای مثال در استاندارد ISO/IEC 20000-1، سازمان فراهم‌کننده خدمت به ندرت همه مخاطرات را بر عهده می‌گیرد. از مشتری انتظار می‌رود تا مخاطرات باقیمانده را به‌عنوان قسمتی از توافقنامه سطح خدمت یا طرح تدوام خدمت بپذیرد. در استاندارد ISO/IEC 27001، موضوع مالکیت مخاطره به روشنی بحث نشده است، اما در عمل سازمان به‌عنوان مالک همه مخاطرات امنیت اطلاعات باقیمانده در نظر گرفته می‌شود. درک اشتباه از گزینه‌های مدیریت مخاطره به دلیل تفاوت در الزامات برای مدیریت مخاطره بین دو استاندارد به وجود می‌آید. وقتی برای پیاده‌سازی یکپارچه هردو استاندارد برنامه‌ریزی می‌شود، توصیه می‌شود سازمان‌ها در فکر هرگونه تفاوت در معیار مخاطره و تأثیری که این تفاوت‌ها بر برطرف سازی مخاطره دارند، باشند.

بهتر است سازمان یکی از دو رویکردی که در زیر توصیف شده است را اتخاذ کند.

الف- یک رویکرد متداول برای مدیریت مخاطره، شامل ارزیابی مخاطره، برای هردو استاندارد جهت اجتناب از دوباره‌کاری، استفاده شود. برای مثال مخاطره از دست دادن قابلیت دسترسی یک دارایی اطلاعاتی ممکن است توسط قسمت‌های متفاوت سامانه مدیریت یکپارچه تسهیم شود. این رویکرد کاراترین رویکرد است زیرا از دوباره‌کاری تلاش‌ها اجتناب می‌کند.

ب- از روشگان ارزیابی مخاطره جداگانه‌ای برای دو استاندارد استفاده شود. اگر این گزینه انتخاب شود، سازمان بهتر است از اصطلاح‌شناسی استفاده کند که بین ارزیابی مخاطره SMS و خدمات و ارزیابی مخاطره از ISMS و امنیت اطلاعات تمایز قائل شود.

جایی که ارزیابی مخاطره و مدیریت مخاطره برای سازمان نقش کلیدی دارند، توصیه می‌شود اولویت به پیاده‌سازی استاندارد ISO/IEC 27001، اختصاص یابد تا از مزایای راهنمای ارزیابی مخاطره و مدیریت مخاطره آن بهره‌برداری شود. هرکدام از گزینه‌ها که انتخاب شود، توصیه می‌شود سازمان از اصطلاح‌شناسی شفاف و سازگاری استفاده کند. این ممکن است نیاز به بیان الزامات از هردو استاندارد به شیوه‌ای متفاوت با نسخه (های) انتشاریافته داشته باشد. هرچند توصیه می‌شود سازمان هنوز قابلیت ردگیری شفاف الزامات در هردو استاندارد را تضمین کند.

۶-۲-۴ تفاوت‌ها در سطوح پذیرش مخاطره

جایی که یک مشتری، داده یا سامانه‌های خود را به‌دست طرف سوم می‌سپارد، ممکن است تفاوت‌هایی بین سطح پذیرش مخاطره مشتری و طرف سوم وجود داشته باشد. این مسئله به طور واضح در هیچ‌کدام از استانداردها پوشش داده نشده است، اما توصیه می‌شود سازمان از این موضوعات آگاه باشد و با توجه به سطح مخاطره که توسط طرف‌های مختلف کنترل می‌شوند، تصمیم روشنی بگیرد.

موضوعات کلیدی در زیر توصیف شده‌اند.

الف- مشتری بر اساس سطح امنیتی قابل‌قبول برای اطلاعات خود که تحت کنترل طرف سوم است، چشم‌اندازی دارد. این چشم‌انداز ممکن است با سطح امنیتی که طرف سوم کافی می‌داند، مطابق نباشد.

ب- همچنین طرف سوم اطلاعات شخصی خود را دارد، برای مثال سوابق مالی. طرف سوم بر اساس سطح امنیتی که برای این اطلاعات قابل‌قبول است چشم‌اندازی دارد.

پ- مشتری و طرف سوم می‌توانند در محیط‌های قانونی و مقررات تنظیم‌شده اجباری متفاوتی که بر اساس کشور یا قسمت بازار متنوع است، درگیر باشند. این مسئله می‌تواند به سمت چشم‌اندازهای امنیت اطلاعات یا مخاطره متفاوتی هدایت کند.

انتظارات و مسئولیت‌های امنیت اطلاعات سازمان مشتری و طرف سوم در اولین فرصت ممکن بهتر است مورد بحث قرار بگیرد. این مذاکرات برای توافق بر محدوده کاربرد پروژه پیاده‌سازی و به همان اندازه برای برقرار کردن کنترل‌های عملیاتی برای خدمات موجود حائز اهمیت است. هرگونه تعارض بالقوه شناسایی‌شده و تصمیمات گرفته شده و توافق به طور ایده‌آل قبل از پیاده‌سازی حاصل شود.

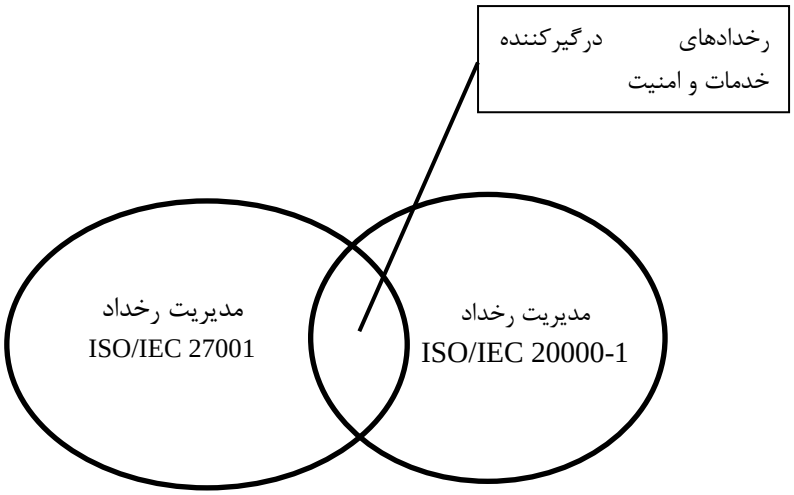
۶-۲-۵ مدیریت رخداد و مشکل

اولین نقطه قابل‌بحث اصطلاح‌شناسی است. در استاندارد ISO/IEC 27001، تنها یک اصطلاح برای رویدادهای ناخواسته مدنظر وجود دارد: رخداد امنیت اطلاعات. در مقابل در استاندارد ISO/IEC 20000-1، اصطلاحات تخصصی فراوانی مرتبط با مدیریت رخداد وجود دارد. برای مثال، رخداد، رخداد امنیت اطلاعات، مشکل، خطای شناخته‌شدهشناخته‌شده و رخداد بزرگ، به پیوست ب از این استاندارد بین‌المللی مراجعه کنید. بر طبق استاندارد ISO/IEC 27001، همه اینها بر اساس ویژگی‌های خود می‌توانند رخدادهای امنیت اطلاعات باشند.

استاندارد ISO/IEC 27001، یک فرآیند واحد را برای رسیدگی کردن به تمام رخدادهای امنیت اطلاعات توصیف می‌کند.

استاندارد ISO/IEC 20000-1، نه تنها دارای اصلاحات متنوعی است، بلکه سازوکارهای گوناگونی برای مدیریت این رویدادها، مانند مدیریت رخداد و تقاضای خدمت، روال رخدادهای بزرگ و مدیریت مشکل را داراست. در استاندارد ISO/IEC 20000-1، یک رویداد ساده می‌تواند توسط بیش از یکی از این فرآیندها و روال‌ها در طول دوره حیاتش مدیریت شود. استاندارد ISO/IEC 20000-1، از تعریف استاندارد ملی ایران به شماره ۹۰۰۰، سال: ۱۳۸۷ برای روال استفاده می‌کند. «روش مشخص‌شده برای انجام یک فعالیت یا فرآیند.» در استاندارد ISO/IEC 20000-1، فرآیند سطح بالاتری نسبت به روال دارد، با روال‌هایی که یک فرآیند را پشتیبانی می‌کنند.

شکل ۳ ارتباط بین مدیریت مخاطره امنیت اطلاعات در استاندارد ISO/IEC 27001 و مدیریت مخاطره در استاندارد ISO/IEC 20000-1 را توصیف می‌کند.



شکل ۳- توصیف ارتباط بین استانداردها برای مدیریت مخاطره

رویدادهایی وجود دارند که استاندارد ISO/IEC 27001، آنها را به‌عنوان رخداد امنیت اطلاعات طبقه‌بندی می‌کند، اما استاندارد ISO/IEC 20000-1، آن را به‌عنوان یک رخداد طبقه‌بندی نمی‌کند. دو مثال در ادامه آورده شده است:

الف- برخلاف خط‌مشی امنیت اطلاعات، یک مستند محرمانه درباره بازاریابی یک محصول، بعد از ساعت کاری روی یک میز پیدا می‌شود. مستند هیچ‌گونه ارتباطی با تحویل خدمت ندارد.

ب- قفل در یک دفتر کار مشتری شکسته پیدا می‌شود. این رویداد تحت استاندارد ISO/IEC 27001، یک رخداد در نظر گرفته می‌شود. هرچند این رویداد درون حوزه استاندارد ISO/IEC 20000-1، قرار نمی‌گیرد مگر اینکه باعث دسترسی به اطلاعات مربوط به الزامات در بند ۶-۶، استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شود.

به همان اندازه رویدادهایی وجود دارند که استاندارد ISO/IEC 20000-1، آنها را به‌عنوان رخداد دسته‌بندی می‌کند، اما خارج از محدوده استاندارد ISO/IEC 27001، قرار دارند. برای مثال:

الف- نگهداری برنامه‌ریزی شده، از محدودیت‌های توافقنامه سطح خدمت تخطی کند.

ب- یک کاربر به دلیل آهسته بودن کارایی خدمت، یک رخداد را گزارش دهد.

هم‌پوشانی اولیه بین تعاریف «رخداد» به آنچه استاندارد ISO/IEC 20000-1، به آن به‌عنوان «رخدادهای امنیت اطلاعات» ارجاع می‌دهد، مربوط است که باعث از دست دادن محرمانگی، یکپارچگی و دسترس‌پذیری مرتبط با خدمت می‌شود.

به‌منظور تطبیق این دیدگاه‌ها، سازمان بهتر است تصمیم بگیرد چگونه مدیریت رخدادها را که در محدوده هردو سامانه مدیریت هستند، ساماندهی کند.

مدیریت مشکل در استاندارد ISO/IEC 20000-1، به‌عنوان فرآیندی برای تشخیص ریشه علت یک یا تعداد بیشتری رخداد برای به حداقل‌رسانی و یا اجتناب از تأثیر رخدادها، تعریف‌شده است. در استاندارد ISO/IEC 20000-1، مدیریت مشکل یک فرآیند جداگانه مشخص است. در استاندارد ISO/IEC 27001، مدیریت

مشکل به روشنی پوشش داده نشده است، هرچند در الزامات مدیریت رخداد امنیت اطلاعات، برطرف سازی مخاطره و کنش‌های اصلاحی، به آن اشاره شده است.

توصیه می‌شود در یک سامانه مدیریت یکپارچه، فرآیند مدیریت مشکل تعریف شود. اگر ISMS قبل از SMS پیاده‌سازی شود، یکپارچه‌سازی بهترین تجارب SMS برای مدیریت مشکل به‌عنوان قسمتی از ISMS به دلیل منافع خود برای همه سامانه‌های مدیریت، می‌تواند مفید باشد.

هر دو استاندارد، سازمان را به تحلیل داده‌ها و روندهای رخداد، الزام می‌کنند.

رخدادهایی که شامل یک مخاطره امنیت اطلاعات می‌شوند، بهتر است به‌عنوان رخدادهای امنیت اطلاعات طبقه‌بندی شوند. به همین نسبت مطابقت با هر دو استاندارد مهم است، به گونه‌ای که فرآیند مدیریت رخداد بهتر است نیاز به انطباق با الزامات مازاد برای امنیت اطلاعات در استاندارد ISO/IEC 27001 را منعکس کند.

بهتر است توجه شود که کنترل در بند ۱۳-۲-۲ از پیوست الف استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، یادگیری از مخاطرات امنیت را پوشش می‌دهد و بنابراین یک هم‌پوشانی جزئی با مدیریت مشکل در بند ۸-۲، استاندارد ملی ایران به شماره ۱-۱۶۳۴۷: سال ۱۳۹۱، است. علاوه بر این شناسایی و ارزشیابی آسیب‌پذیری‌های مورد نیاز برای یک ارزیابی مخاطره امنیت اطلاعات در استاندارد ISO/IEC 27001، توصیه می‌شود به‌عنوان یک فرآیند تحلیل داده که می‌تواند به‌عنوان ورودی مدیریت مشکل به‌کار رود، در نظر گرفته شود.

موضوع دوم توصیف مسئله پاسخگویی به رخداد است. توصیه می‌شود هر سازمانی دارای هدف بازسازی سریع خدمت بعد از اینکه رخداد امنیت اطلاعات یک خدمت را تحت تأثیر قرارداده است، باشد. هرچند این عمل می‌تواند احتمال بررسی مخاطره امنیت را جهت یافتن دلیل آن کاهش دهد. زمانی که یک SMS و یک ISMS یکپارچه می‌شوند، بهتر است مراقب بود تا الزامات برای مدیریت مخاطرات امنیت اطلاعات مطابق باشند. برای مثال کنترل‌های امنیت اطلاعات می‌توانند شامل جمع‌آوری، نگهداری و فراهم کردن مدرک برای اهداف انتظامی یا قانونی شوند. علاوه بر آن هردو استاندارد ملتزم به انطباق با الزامات قانونی و مقررات تنظیم‌شده می‌باشند.

توصیه می‌شود این موضوع به رسمیت شناخته شود که در مورد رخداد امنیت اطلاعات، نیاز به جمع‌آوری مدرک می‌تواند بدین معنا باشد که خدمت تحت تأثیر نمی‌تواند درون محدوده اهداف خدمت توافق شده، بازسازی شود. استاندارد ملی ISO/IEC 20000-1، فراهم‌کننده خدمت را ملزم به در نظر گرفتن فوریت و اثر رخداد می‌کند. این بدین معناست که زمان بیشتری قبل از برطرف شدن رخداد امنیت اطلاعات مورد نیاز است. اولویتی که به حل رخداد اختصاص می‌یابد بهتر است اهمیت جمع‌آوری مدرک امنیت اطلاعات را در نظر بگیرد، در غیر این صورت مدرک با بازسازی خدمت از بین می‌رود.

در برخی موارد رخداد امنیت اطلاعات، بر اساس تعریف توافق شده رخداد بزرگ با مشتری تحت بند ۸-۱ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، یک رخداد بزرگ است. بر اساس الزامات گزارش‌گیری خدمت در بند ۶-۲ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱ و الزامات مدیریت رخداد بزرگ در بند ۸-۱ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مدیریت ارشد باید در جریان تمام

رخدادهای بزرگ قرار بگیرد. این شامل مواردی که که مخاطرات امنیت اطلاعات هستند نیز می‌شود. این عمل اطمینان می‌دهد که یک شخص صحیح تربیت شده و معتبر برای مدیریت یک رخداد امنیت اطلاعات منصوب شده است. توصیه می‌شود در سامانه مدیریت یکپارچه این رویداد به‌عنوان رخداد بزرگ مدیریت - شود.

توصیه نمی‌شود رخداد بزرگ به طور معمول به گونه‌ای اعلان شود که برای جمع‌آوری مدرک در مورد یک رخداد امنیت اطلاعات، باعث تأخیر در حل رخداد شود. برای مثال اگر یک وب سایت که پرداخت مشتری را ساماندهی می‌کند، به خطر بیفتد. زمان جمع‌آوری مدرک و بازسازی خدمت بهتر است در کالانمای خدمات در الزامات خدمت و در توافقنامه سطح خدمت به طور مناسب پوشش داده شود.

تعریف امنیت اطلاعات در استاندارد ISO/IEC 20000-1، کلمه «دسترس‌پذیری» را به‌کار می‌برد و استاندارد ISO/IEC 27001، از کلمه «قابلیت‌دسترسی» استفاده می‌کند. این تفاوت به این دلیل است که کلمه «قابلیت دسترسی» همان طور که در پیوست ب توصیف شده، در دو استاندارد متفاوت تعریف‌شده است.

۶-۲-۶ مدیریت تغییر

بندهای ۱۰-۱-۲ و ۱۲-۵-۱ در پیوست الف از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، مدیریت تغییر را توصیف می‌کنند. این دو بند هر دو به سازمان اجازه می‌دهند که روال‌ها را جهت برآوردن نیازهای ویژه بهبود بخشند.

بند ۹-۲ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مدیریت تغییر، شامل الزامات مرتبط با مخاطره است. این الزامات توسط بند ۶-۶-۳، تغییرات و رخدادهای امنیت اطلاعات، تکمیل می‌شوند. بند ۶-۶-۳ شامل الزامات برای ارزیابی اثر تغییرات درخواست شده است تا تأثیر آنها بر کنترل‌های امنیت اطلاعات موجود در نظر گرفته شود.

برای اطمینان از اینکه نیازمندی‌های مدیریت تغییر برآورده می‌شود، بازبینه‌های[1] ارزیابی اثر یا بازنگری پس از پیاده‌سازی بهتر است به‌عنوان قسمتی از سامانه مدیریت یکپارچه بر اساس استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، توسعه داده شود. توصیه می‌شود به‌عنوان قسمتی از فرآیند مدیریت تغییر اطمینان حاصل شود که همه انواع مخاطرات امنیت اطلاعات مورد بازنگری قرارگرفته‌اند.

۶-۳ فواید بالقوه

۶-۳-۱ استفاده از چرخه طرح-اجرا- بررسی-اقدام

استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، هردو به وضوح به چرخه طرح-اجرا-بررسی-اقدام[2] (PDCA) ارجاع داده‌اند. هرکدام از استانداردها که بخواهند اول پیاده‌سازی شوند سازمان می‌تواند اصول یکسانی را دنبال کند و این می‌تواند کار را راحت کند.

1- Checklists
2- Plan-Do-Check-Act (PDCA)

چرخه PDCA اساس بهبود مستمر در هر دو استاندارد است، بنابراین بهبود مستمر در زمان پیاده‌سازی یک یا هردو استاندارد بهتر است مرکز توجه فعالیت‌ها باشد. بهتر است در نظر داشت که چرخه‌های PDCA می‌توانند در مقیاس زمانی مختلف اتفاق بیفتد، اما اگر در کل ممکن باشد سازمان بهتر است یک چرخه واحد یکپارچه برای فراهم کردن دوره بازنگری یا ممیزی داخلی یکنواخت را به‌کار برد.

۶-۳-۲ مدیریت سطح خدمت و گزارش‌گیری

گزارش‌گیری خدمت پایه گسترده‌تری از فعالیت‌ها را نسبت به فعالیت‌های مورد نیاز مدیریت سطح خدمت پوشش می‌دهد. هرچند گزارش‌گیری خدمت می‌تواند مدیریت امنیت اطلاعات را با داشتن اهداف خدمت برای رخدادهای امنیت اطلاعات که سنجش‌شده، گرایشی پیدا کرده و در گزارش‌گیری خدمت استفاده شده است، پشتیبانی کند.

مورد ب از بند ۶-۲ در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بیان می‌دارد که فرآیند گزارش‌گیری خدمت بهتر است شامل اطلاعات مرتبط با رویدادهای مهم باشد، مانند رخدادهای بزرگ و عدم انطباق‌ها. خروجی‌ها از فرآیند گزارش‌گیری خدمت در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، می‌تواند یک مزیت بزرگ برای نگهداری و بهبود امنیت اطلاعات باشد.

وقتی استاندارد ISO/IEC 27001، پیاده‌سازی می‌شود، جزئیات کنترل‌های امنیت اطلاعات تعریف‌شده‌هشده است و اثربخشی این کنترل‌ها باید سنجش شود؛ به بند ۴-۲-۳، پایش و بازنگری ISMS، از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، مراجعه کنید. این عمل همچنین یک فرصت برای یکپارچه شدن با بند ۶-۲ فرآیند گزارش‌گیری خدمت در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، فراهم می‌کند، اطلاعات مرتبط و بهنگام می‌تواند برای نگهداری یا بهبود امنیت اطلاعات به‌کار رود. مشتریان می‌توانند درک بهتری از کارایی درست خدمات و SMS، شامل فرآیندهای مدیریت خدمت داشته باشند، اگر سطوح انطباق کنترل امنیت اطلاعات مرتبط و آمار رخداد در گزارش گنجانیده شود.

گزارش‌های استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1، چه برای استفاده داخلی و چه برای مشتریان، بهتر است با در نظر گرفتن این ملاحظات طراحی شوند.

۶-۳-۳ تعهد مدیریتی

استاندارد ISO/IEC 27001، امنیت اطلاعات در رابطه با ذی‌نفعان را توصیف می‌کند. ذی‌نفعانی که به آنها اشاره شده است طرف‌هایی هستند، با نفع واگذارشده در سازمانی که ISMS در آن پیاده‌سازی شده است. این طرف‌ها می‌توانند شامل کارمندان، سهامداران، مشتریان و احتمالاً حتی مقامات نظارتی یا عموم مردم شوند. استاندارد ISO/IEC 20000-1، به مشتریان و طرف‌های ذی‌نفع اشاره می‌کند. طرف‌های ذی‌نفع شخص یا گروهی هستند که سود خاصی در کارایی یا موفقیت فعالیت یا فعالیت‌های فراهم‌کننده خدمت دارند؛ بنابراین طرف‌های علاقه‌مند مشابه «ذی‌نفعان» که در استاندارد ISO/IEC 27001، استفاده شده است، می‌باشند.

تعهد مدیریت ارشد برای ایجاد SMS کارا الزامی است. این مسئله شامل اطمینان از اینکه ارتباطات بین مشتری و سایر طرف‌های ذی‌نفع موفق است، است. به همین ترتیب تعهد مدیریت که در استاندارد ملی

ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، بیان شده است، از رویکرد متمرکز مشتری در استاندارد ISO/IEC 20000-1، پشتیانی می‌کند.

استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، الزامات ویژه برای تعهد و مسئولیت‌های مدیریتی را شامل می‌شود، برای مثال الزامات در بندهای ۴-۱-۱ و ۴-۱-۴. در مقابل استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، درباره اینکه کدام نقش‌ها بهتر است مسئول و پاسخگو برای ISMS باشند، کمتر مورد توجه است، برای مثال الزامات ۵-۱ و ۵-۲-۲. یک سامانه مدیریت یکپارچه بهتر است مزایای ماهیت استاندارد ISO/IEC 20000-1 را دریافت کرده و از الزامات آن بهره‌برداری کند تا اطمینان حاصل شود که مسئولیت‌های گسترده‌تر امنیت اطلاعات به‌اندازه مسئولیت‌های مدیریت خدمت جدی گرفته می‌شود.

استاندارد ISO/IEC 20000-1، بیان می‌دارد که در هنگام ارائه مدیریت بهبودها، سازمان بهتر است مسئولیت را برای مدیریت فرآیند بهبود به یک نقش خاص واگذار کند. برعکس بندهای ۴-۲-۴ و ۸-۱ از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، به سازمانی که این وظیفه را سازمان‌دهی می‌کند اشاره دارد، درحالی‌که بند ۵-۱ شامل الزاماتی است که سازمان برای برپا کردن نقش‌ها و مسئولیت‌ها برای امنیت اطلاعات دارد. توصیه می‌شود الزامات استاندارد ISO/IEC 20000-1، برای انتصاب واضح مسئولیت‌ها جهت مدیریت بهبود به‌کار رود تا اطمینان حاصل شود که مدیریت بهبود برای امنیت اطلاعات به نقش مشخصی تخصیص یافته است.

۶-۳-۴ مدیریت ظرفیت

مدیریت ظرفیت در بند ۶-۵ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل طیف وسیع‌تری از مفاهیم ظرفیت نسبت به استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، است، بنابراین برخی الزامات استاندارد ISO/IEC 20000-1، برای پشتیبانی پیاده‌سازی استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، می‌تواند به‌کار رود. برای مثال، مدیریت ظرفیت که در استاندارد ISO/IEC 20000-1، توصیف شده است، به ظرفیت فنی و ظرفیت منابع انسانی، هردو اعمال می‌شود. علاوه بر آن، از آنجایی‌که ظرفیت، دسترسی به منابع کافی جهت رسیدگی به شرایط قابل پیش‌بینی معقولانه تعریف می‌شود، در بند ۵-۲ از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، مدیریت منابع، می‌تواند به مدیریت ظرفیت مرتبط شود.

در بند ۳-۲ از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، در قابلیت دسترسی، دست‌یافتنی و قابل‌استفادهقابل‌استفاده بودن تعریف می‌شود. در بند ۶-۵ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مدیریت ظرفیت هر دو بعد از قابلیت دسترسی را پشتیبانی می‌کند. برای مثال، اگر ظرفیت کافی وجود نداشته باشد، یک خدمت یا قسمتی از خدمت می‌تواند دست‌نیافتنی باشد، مثلاً اگر ذخیره یک پرونده به دلیل ظرفیت ذخیره‌سازی بسیار کم ممکن نباشد. متناوباً، یک خدمت یا جزئی از خدمت می‌تواند بسیار کند و بنابراین غیرقابل‌استفاده باشد، برای مثال زمان پاسخ به دلیل ظرفیت شبکه بسیار کم.

توصیه می‌شود سازمان هنگام ارجاع متقابل الزامات بین استانداردها، از این تفاوت‌ها آگاه باشد. سازمان بهتر است نیاز به ارجاع متقابل بندهای ۴-۳ و ۶-۵ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱ و بندهای مربوط در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷ را در نظر بگیرد، به پیوست الف از این استاندارد بین‌المللی مراجعه کنید. برای مثال الزام به شمول اثر بالقوه تغییرات قانونی، مقرراتی، قراردادی یا

سازمانی در طرح ظرفیت که توسط بند ۶-۵ استاندارد ملی ایران بـه شـماره ۱-۱۶۳۴۷ سـال:۱۳۹۱، الـزام شده است، بهتر است با بند الف-۱۰-۱ از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، ارجاع متقابـل شود.

۶-۳-۵ مدیریت مخاطرات طرف سوم

در استاندارد ISO/IEC 27001، یک طرف سوم، مانند مشتری، تأمین‌کننده یا گروه داخلی مستقل، خارج از محدوده ISMS وجود دارد و به‌عنوان منبعی بالقوه از مخاطره دیده می‌شـود. پیوسـت ب از ایـن اسـتاندارد بین‌المللی شامل یک مقایسه از این اصطلاحات است، استاندارد ISO/IEC 27001، کنترل‌هایی را کـه مـی-توانند برای مدیریت امنیت این طرف سوم‌ها به‌کار روند در بند الـف-۶-۲-۱ و الـف-۶-۲-۳ توصـیف کـرده است.

در مقابل در استاندارد ISO/IEC 20000-1، طرف سوم‌ها موجودیت‌هایی هستند که تحت کنتـرل مسـتقیم فراهم‌کننده خدمت نیستند، اما در محدوده SMS با خدمت همکاری می‌کنند. سایر طرف‌ها تأمین‌کنندگان، گروه‌های داخلی یا مشتریان (وقتی که به‌عنوان تأمین‌کننده عمل می‌کنند) هستند. سایر طرف‌ها می‌تواننـد با قسمت بزرگی از خـدمت همکـاری کننـد، بـه بنـد ۴-۲ از اسـتاندارد ملـی ایـران بـه شـماره ۱-۱۶۳۴۷ سال:۱۳۹۱، نظارت بر فرآیندهایی که توسط سایر طرف‌ها[1] اجرا می‌شوند، مراجعه کنید. بند ۶,۶ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، الزامات برای مدیریت امنیت اطلاعات را توصیف مـی‌کنـد. ایـن توصیف شامل مدیریت مخاطرات مرتبط با تأمین‌کننده است کـه مـی‌توانـد مسـتقیماً بـر امنیـت اطلاعـات سازمان مشتری تأثیر بگذارد. همچنین بند ۸-۱ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بـه فرآیند رخداد و تقاضای خدمت برای مدیریت رخدادهای امنیـت اطلاعـات و ارزیـابی همـه تغییـرات بـرای بازنگری تأثیر بر کنترل‌های امنیت اطلاعات، ارجاع می‌دهد.

وقتی یک سامانه مدیریت یکپارچه طراحی می‌شود، دو ملاحظه اصلی که بر روابط کسب‌وکـار و فرآینـدهای مدیریت تأمین‌کننده با توجه به مدیریت مخاطرات طرف سوم تأثیر می‌گذارد، وجـود دارنـد. دو ملاحظـه در زیر توصیف شده‌اند:

الف- تعهدات امنیت اطلاعات قراردادی بهتر است یک ورودی برای فرآیند ارزیابی مخاطره باشـند. توصـیه می‌شود این فرآیند برای انجام الزامات استاندارد ISO/IEC 20000-1، برای فراهم‌کننده خدمت برای پاسخ به نیازهای کسب‌وکار همکاری کند.

ب- وقتی در تعامل با سایر طرف‌ها، شامل مشتریانی که به‌عنوان تأمین‌کنندگان عمل می‌کننـد، هسـتیم بهتر است امنیت اطلاعات پوشش داده شود. توصیه می‌شود این مسئله وقتی یک خـدمت جدیـد یـا تغییریافته طراحی شده است و کالانمای خدمت و توافقنامه‌های سطح خدمت بحث می‌شود، در نظر گرفته شود.

سایر مفاهیم که در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بنـد ۷-۱ پوشـش داده شـده‌انـد، مانند بازنگری‌های کارایی، تغییرات خدمت، مدیریت رضایت مشتری و ساماندهی شکایات، می‌تواند به سامانه مدیریت یکپارچه اعمال شود تا آن را در کل تقویت کند.

1- Parties

به طور خلاصه سامانه مدیریت یکپارچه بهتر است رویکرد استاندارد ISO/IEC 27001 را برای مدیریت روابط با تأمین‌کنندگان دنبال کند، اما همچنین با الزامات بند ۶-۶-۲ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، کنترل‌های امنیت اطلاعات با توجه به مخاطره تأمین‌کننده، انطباق یابد. در جایی که دارایی‌های سازمان درون محدوده ISMS قرار می‌گیرد اما برخی یا همه این دارایی‌ها توسط طرف دیگری کنترل می‌شود، توصیه می‌شود سازمان بر روی قراردادهای مناسب، توافقنامه‌های سطح خدمت یا سایر توافقنامه‌های مستند شده، توافق کند. این رویکرد بهتر است تضمین کند که طرف سوم یا سایر طرف‌ها کنترل‌های مناسبی اعمال می‌کنند.

۶-۳-۶ مدیریت تداوم و قابلیت دسترسی

بند ۶-۳ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، (در رابطه با) مدیریت تداوم و قابلیت دسترسی، به طور واضح یک قسمت از نواحی مهم امنیت اطلاعات را پوشش می‌دهد. تداوم و قابلیت دسترسی فعالیت‌ها در سامانه مدیریت موجود بهتر است بازنگری شود تا دریابیم آیا آنها می‌توانند به طرز مفیدی برای پوشش دادن مدیریت یکپارچگی و محرمانگی گسترش داده شوند و بنابراین امنیت اطلاعات برای هر خدمتی را مدیریت کنند. در اینجا جزئیات می‌توانند از استاندارد ISO/IEC 20000-1 و اصول عمومی از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، بند الف-۱۴ استخراج شوند.

۶-۳-۷ مدیریت تأمین‌کننده

استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، مدیریت تأمین‌کننده را در بندهای مختلف مانند الف-۶-۲-۱، الف-۶-۲-۳، الف-۱۰-۲، الف-۸ برای منابع انسانی شامل پیمانکاران پوشش می‌دهد. بند ۴-۲ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل الزامات برای نظارت بر فرآیندهایی که توسط سایر طرف‌ها اجرا می‌شوند، است و بند ۷-۲ شامل الزامات برای مدیریت تأمین‌کننده است. مدیریت تأمین‌کننده تحت هر دو استاندارد می‌تواند به طور مؤثری ترکیب شوند.

بند ۶-۳-۵ از این استاندارد بین‌المللی شامل اطلاعات بیشتری در رابطه با مدیریت مخاطرات مرتبط با تأمین‌کننده است. برای مثال ارزیابی مخاطره در استاندارد ISO/IEC 20000-1، می‌تواند با به‌کارگیری مفاهیم استاندارد ISO/IEC 27001، گسترش یابد تا ملاحظه شود آیا امنیت سازمان با اضافه یا حذف کردن یک تأمین‌کننده، یا با تغییر خاص در خدمتی که تأمین‌کننده در آن همکاری دارد، به خطر می‌افتد یا خیر. حتی اگر سازمان تصمیم بگیرد تنها یک استاندارد را پیاده‌سازی کند این موارد بهتر است در نظر گرفته شود.

۶-۳-۸ مدیریت پیکربندی

انبار دارایی در استاندارد ISO/IEC 27001، مخزنی از هر چیزی است که برای سازمان دارای ارزش[1] (پولی یا غیره) است و در محدوده کاربرد ISMS وجود دارد، مانند اطلاعات، دادگان[2] یا فرآیندها.

1- value
2- DataBases

مفهوم دادگـان مـدیریت پیکربنـدی در اسـتاندارد ISO/IEC 20000-1، مشـابه انبـار دارایـی در اسـتاندارد ISO/IEC 27001، است؛ اما محدوده و بنابراین چشم‌انداز آن متفاوت است. پیاده‌سازی محدوده در بنـد ۴-۱-۵ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مورد بحث قرار گرفته است.

الزامات در بند ۹-۱ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، می‌توانـد در ایجـاد و مـدیریت یک ISMS به‌کار رود. از منظر استاندارد ISO/IEC 27001، توصیه می‌شود سازمان امنیت دادگان مـدیریت پیکربندی را مدیریت کند که این کار بهتر است به‌عنوان یک دارایی اطلاعات مدنظر قرار بگیرد.

همچنین بند ۹-۱ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، ملزم می‌کند که دادگان مدیریت پیکربندی امن باشد تا درستی داده‌های نگاه داشته شده، حفـظ شـود. ایـن عمـل الزامـاتی بـرای نگهـداری خدمات و یکپارچگی اجزا خدمت را شامل می‌شـود. هرچنـد اسـتاندارد ISO/IEC 20000-1، تمـایزی بـین سطوح مختلف یکپارچگی ترسیم نمی‌کند. در اینجا استاندارد ISO/IEC 27001، می‌تواند ارزش اضافه کنـد، زیرا الزام می‌کند که مخاطرات سامانه‌ها، خدمات و اجـزا خـدمت ارزشـیابی شـوند و سـطوح قابـل‌قبـولی از مخاطره تعریف شود. مسئله اصلی این است که آیا سطح مخاطره ممکن است با تغییـر، عـوض شـود و اگـر چنین است آیا این عوض شدن مخاطره را تا سطح غیرقابل‌قبولی بالا می‌برد.

الزامات جهت مبنای پیکربندی و نسخه‌های اصلی در استاندارد ISO/IEC 20000-1، عملاً از منظر استاندارد ISO/IEC 27001، کنترل می‌شود. این الزامات بهتر است هنگام یکپارچه‌سازی رویکردهای مدیریت مخاطره در نظر گرفته شود. برخی از آنها بر تصمیم بر اینکه آیا برخی کنترل‌ها پیاده‌سازی شوند یا خیر تـأثیر مـی-گذارد.

۹-۳-۶ مدیریت انتشار و استقرار

مطابقت با الزامات مدیریت انتشار و اسـتقرار در بنـد ۹-۳ در اسـتاندارد ملـی ایـران بـه شـماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مطابقت با الزامات استاندارد ISO/IEC 27001، برای انتشار را تضمین نمـی‌کنـد. اگـر الزامـات استاندارد ISO/IEC 27001، دنبال نشده باشند برخی مسائل امنیتی ممکن اسـت بـه طـور اتفـاقی در ایـن مرحله وارد شوند. برای مثال:

الف- اگر مدیریت انتشار و استقرار احتمال کنش بدخواهانه را در نظر نگیـرد، در عملکـرد سـامانه (هـای) واقعی که نقص‌های امنیت اطلاعات را وارد می‌کنند، می‌تواند تغییرات ایجاد شود.

ب- مدیریت آزمون و مدیریت محیط واقعی اغلب توسط گروه‌های متفاوت انجام می‌شود، بنـابراین یـک فرآیند انتشار بهتر است تضمین کند که نقش تولید درست داده‌ها را از گروه آزمون دریافت می‌کند، برای جلوگیری از مخاطرات داده‌های محرمانه.

این مسئله به طور ویژه در طول انتشارهای اضطراری اهمیت می‌یابد. در این موقعیت‌ها، به دلیل محدودیت-های زمان و/یا منابع، اغلب یک انتشار و استقرار متفاوت و احتمالاً موقت به‌کار می‌رود؛ بنابراین مخاطرات، به خطر افتادن امنیت اطلاعات افزایش می‌یابد. مخاطرات امنیت اطلاعات بهتر است همیشـه بـا دنبـال کـردن فرآیندهای امنیت اطلاعات تأییدشده، بدون توجه به اینکه کدام فرآیند انتشار و استقرار استفاده می‌شود، به خوبی مدیریت شوند.

مدیریت انتشار و استقرار می‌تواند از طریق انتخاب کنترل‌ها در الف-۱۰-۱-۴ در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، جدا از توسعه، آزمون و تسهیلات عملیاتی و الف-۱۰-۳-۲، پذیرش سامانه، بهبود یابد.

۶-۳-۱۰ بودجه‌بندی و حسابداری

الزامات بودجه‌بندی و حسابداری در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بند ۶-۴، نمی-تواند به طور مستقیم به هیچ یک از الزامات استاندارد ISO/IEC 27001، نگاشت شود. در استاندارد ISO/IEC 27001، الزام فراهم کردن منابع و خروجی بازنگری مدیریت (که نیازمند تصمیمی است که باید در رابطه با نیازهای منابع گرفته شود) می‌تواند از فرآیند ملاحظه منابع مالی و یک بودجه تعریف‌شده بهره ببرد.

پیوست الف

(اطلاعاتی)

تشابه بین استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷ و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱

الف- ۱ کلیات

پیوست الف مقایسه‌ای در سطح بند از محتوای استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷ و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، ارائه می‌دهد.

بندهایی که در بیشتر الزامات و جزئیات در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷ و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، هم‌پوشانی دارند، به رنگ خاکستری روشن مشخص‌شده‌اند.

بندهایی که در بیشتر الزامات و جزئیات در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، پیوست الف و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، هم‌پوشانی دارند، به رنگ خاکستری تیره مشخص‌شده‌اند.

نواحی بدون سایه آنهایی هستند که هم‌پوشانی قابل‌توجهی ندارند.

جدول الف ۱- تشابه بین استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷ و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱

استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱
مقدمه	مقدمه
کلیات	بدون معادل مستقیم
رویکرد فرآیندی	بدون معادل مستقیم
سازگاری با سایر سامانه‌های مدیریت	بدون معادل مستقیم
۱ محدوده کاربرد	۱ محدوده کاربرد
۱-۲ کلیات	۱-۲ کلیات
۱-۲ کاربرد	۱-۲ کاربرد
۲ مراجع الزامی	۲ مراجع الزامی
۳ اصطلاحات و تعاریف	۳ اصطلاحات و تعاریف
۴ سامانه مدیریت امنیت اطلاعات	۴ الزامات عمومی سامانه مدیریت خدمت
۴-۱ الزامات عمومی	بدون معادل مستقیم
۴-۲ برقراری و مدیریت **ISMS**	۴-۵ برقراری و مدیریت **SMS**
بدون معادل مستقیم	۴-۵-۱ تعریف محدوده کاربرد
بدون معادل مستقیم	۴-۵-۲ برنامه‌ریزی **SMS** (برنامه‌ریزی)

استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱
۴-۲-۲ پیاده‌سازی و اجرای **ISMS**	۴-۵-۳ پیاده‌سازی و اجرای **SMS** (اجرا)
۴-۲-۳ پایش و بازنگری **ISMS**	۴-۵-۴ پایش و بازنگری **SMS** (بازبینی)
۴-۲-۴ نگهداری و بهبود **ISMS**	۴-۵-۵ نگهداری و بهبود **SMS** (انجام)
۴-۳ الزامات مستندسازی	۴-۳ مدیریت مستندسازی
۴-۳-۱ کلیات	۴-۳-۱ برقراری و نگهداری مستندات
۴-۳-۲ کنترل مستند	۴-۳-۲ کنترل مستندات
۴-۳-۳ کنترل سوابق	۴-۳-۳ کنترل سوابق
۵ مسئولیت مدیریت	۴-۱ مسئولیت مدیریت
۵-۱ تعهد مدیریت	۴-۱-۱ تعهد مدیریت
بدون معادل مستقیم	۴-۱-۲ خط مشی مدیریت خدمت
بدون معادل مستقیم	۴-۱-۳ اختیار، مسئولیت، ارتباط
بدون معادل مستقیم	۴-۱-۴ نماینده مدیریت
بدون معادل مستقیم	۴-۲ نظارت بر فرآیندهایی که توسط سایر همکاران انجام می‌گیرد
۵-۲ مدیریت منابع	۴-۴ مدیریت منابع
۵-۲-۱ فراهم کردن منابع	۴-۴-۱ فراهم کردن منابع
۵-۲-۲ آموزش، آگاه‌سازی و شایستگی	۴-۴-۲ منابع انسانی
۶ ممیزی داخلی **ISMS**	۴-۴-۵-۲ ممیزی داخلی
۷ بازنگری مدیریتی **ISMS**	۴-۴-۵-۳ بازنگری مدیریت
۷-۱ کلیات	۴-۴-۵-۳ بازنگری مدیریت
۷-۲ بازنگری ورودی	۴-۴-۵-۳ بازنگری مدیریت
۷-۳ بازنگری خروجی	۴-۴-۵-۳ بازنگری مدیریت
۸ بهبود **ISMS**	۴-۵-۵ نگهداری و بهبود **SMS**(اجرا)
۸-۱ بهبود مستمر	۴-۵-۵-۱ کلیات
	۴-۵-۵-۲ مدیریت بهبودها
۸-۲ کنش اصلاحی	۴-۵-۵-۱ کلیات
	۴-۵-۵-۲ مدیریت بهبودها
	۸ فرآیندهای تشخیص
۸-۳ کنش پیشگیرانه	۴-۵-۵-۱ کلیات
	۴-۵-۵-۲ مدیریت بهبودها
	۸ فرآیندهای تشخیص
بدون معادل مستقیم	۵ طراحی و انتقال خدمات جدید یا تغییریافته
بدون معادل مستقیم	۵-۱ کلیات
بدون معادل مستقیم	۵-۳ طراحی و توسعه خدمات جدید یا تغییریافته
بدون معادل مستقیم	۵-۴ انتقال خدمات جدید یا تغییریافته
بدون معادل مستقیم	۶ فرآیندهای تحویل خدمت

استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱
الف-۱۰-۲- ۱ تحویل خدمت	۶-۱ مدیریت سطح خدمت
الف-۱۰-۲-۲ پایش و بازنگری خدمات طرف سوم	۶-۲ گزارش‌گیری خدمت
بدون معادل مستقیم	۶-۳ تداوم خدمت و مدیریت قابلیت دسترسی
بدون معادل مستقیم	۶-۴ بودجه‌بندی و حسابداری خدمات
الف-۱۰-۳-۲ مدیریت تغییرات خدمات طرف سوم	۵-۲ برنامه‌ریزی خدمات جدید یا تغییریافته
الف-۱۰-۳-۱ مدیریت ظرفیت	۶-۵ مدیریت ظرفیت
ISO/IEC 27001	۶-۶ مدیریت امنیت اطلاعات
بدون معادل مستقیم	۷ فرآیندهای ارتباطی
بدون معادل مستقیم	۷-۱ مدیریت ارتباطات کسب‌وکار
بدون معادل مستقیم	۷-۲ مدیریت تأمین‌کنندگان
الف-۱۳ مدیریت رخداد امنیت اطلاعات	۸-۱ مدیریت رخداد و تقاضای خدمت
بدون معادل مستقیم	۸-۲ مدیریت مشکل
بدون معادل مستقیم	۹ فرآیندهای کنترلی
بدون معادل مستقیم (به طور جزئی در برخی کنترل‌ها)	۹-۱ مدیریت پیکربندی
الف-۱۲-۵-۱ فرآیندهای کنترل تغییر	۹-۲ مدیریت تغییر
بدون معادل مستقیم	۹-۳ مدیریت انتشار و چیدمان
پیوست الف اهداف کنترلی و کنترل‌ها	(به تفصیل در بالا پوشش داده شده، جزئیات تفکیک را مشاهده کنید)
پیوست ب اصول OECD[1] و این استاندارد بین‌المللی	بدون معادل مستقیم
پیوست پ تشابه بین ISO 9001:2000، ISO 14001:2004 و این استاندارد	بدون معادل مستقیم

1- Organization of Economic Corporation Development

پیوست ب

(اطلاعاتی)

مقایسه اصطلاحات استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱، و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱

در جدول ب-۱ برای حفظ اختصار به استانداردهای بین‌المللی بدون ذکر سال انتشار در ستون «توضیحات کاربرد اصطلاحات در هر دو استاندارد» اشاره شده است. جدول ب-۱ مقایسه‌ای از اصطلاحاتی که در استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱، تعریف‌شده‌اند و واژه‌نامه استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷است و اصطلاحاتی را که در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، تعریف و به‌کاربرده شده است، ارائه می‌دهد. نواحی که اصطلاحات بین ISO/IEC 27000 و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به‌صورت متفاوت تعریف‌شده‌اند، به رنگ خاکستری روشن مشخص شده است.

جدول ب ۱- مقایسه اصطلاحات

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
کنترل دسترسی	۲-۱ اطمینان از دسترسی به دارایی‌ها (۲-۳) به‌صورت مجاز و محدود بر اساس الزامات امنیتی و الزامات کسب‌وکار.	تعریف‌نشده	بدون معادل مستقیم
پاسخگویی	۲-۲ مسئولیت هر هستار در قبال کنش‌ها و تصمیماتش.	تعریف‌نشده	کلمه پاسخگویی در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در معنای انگلیسی معمول خود به‌کار می‌رود: مسئولیت، اجبار به توضیح یا دفاع از کنش‌ها یا رفتارهای شخص، تصدیق یا تعهد مسئولیت. کلمه پاسخگویی برای الزامات در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در بند ۴-۲ ضروری است. یعنی

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			«...توسط... یک نمایش پاسخگویی برای فرآیندها و مجوز برای الزام الصاق به فرآیندها؛»
دارایی	۳-۲ هر آنچه که برای سازمان ارزش دارد. یادآوری: انواع مختلفی از دارایی‌ها وجود دارند، ازجمله: الف- اطلاعات (۲-۱۸)؛ ب- نرم‌افزار، مانند برنامه‌ی رایانه‌ای؛ پ- دارایی فیزیکی، مانند رایانه؛ ت- خدمات؛ ث- افراد، صلاحیت‌ها، مهارت‌ها و تجربیات آن‌ها؛ و ج- دارایی‌های نامشهود، مانند وجهه و شهرت.	تعریف‌نشده	کلمه دارایی در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در معنای انگلیسی معمول خود به‌کار می‌رود: هر چیزی که ارزشمند و مفید درنظرگرفته شود، مانند یک مهارت، کیفیت، شخص، غیره. در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، دفعات کمی از کلمه دارایی استفاده شده است: بند ۴-۱-۴: «[نماینده مدیریت] دارای اختیار و مسئولیت است، شامل: پ- اطمینان از اینکه دارایی‌ها شامل مجوزها که برای تحویل خدمات استفاده می‌شود، بر اساس الزامات قانون مدون و قوانین تنظیم‌شده و تعهدات قراردادی، مدیریت می‌شوند؛ بند ۶-۴»: باید خط‌مشی‌ها و روال‌های مستند شده‌ای برای (آ) بودجه‌بندی و حسابداری برای اجزای خدمت شامل حداقل: ۱)دارایی‌ها-شامل مجوزها-جهت فراهم کردن خدمات؛ وجود داشته باشد. بند ۶-۶-۲: فراهم‌کننده خدمت باید کنترل‌های امنیت فیزیکی،

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			اداری و فنی را جهت: الف- حفظ محرمانگی، یکپارچگی و قابلیت دسترسی دارایی‌های اطلاعاتی؛ پیاده‌سازی و اجرا کند. بند ۹-۱: «باید یک رابط تعریف‌شده بین فرآیند مدیریت پیکربندی و فرآیند مدیریت دارایی مالی وجود داشته باشد. یادآوری: محدوده فرآیند مدیریت پیکربندی مدیریت دارایی مالی را در بر نمی‌گیرد.»
حمله	۲-۴ تلاش جهت تخریب، افشا، دست‌کاری، از کار انداختن، سرقت یا دسترسی غیرمجاز از یک دارایی (۲-۳)	تعریف‌نشده	بدون معادل مستقیم
احراز هویت	۲-۵ ارائه تضمینی که مشخصه ادعاشده هستار درست است.	تعریف‌نشده	ارتباط مستقیم با این اصطلاح مرتبط با امنیت اطلاعات ندارد، «احراز هویت»؛ که در ISO/IEC 270001 در معنای فنی به‌کار رفته است. «احراز هویت» مشابه «درستی سنجی» در فعالیت‌های چرخه حیات سامانه مدیریت نیست.
اصالت‌سنجی	۲-۶ ویژگی که یک هستار همان است که ادعا می‌کند.	۳-۱۱ **یادآوری ۱-** علاوه بر آن، سایر ویژگی‌ها مانند اصالت، پاسخگویی، انکارناپذیری و قابلیت اطمینان نیز می‌تواند مطرح شود.	در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، ارجاع داده شده است اما پس از آن استفاده نشده است.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
دسترس‌پذیری	۲-۷ ویژگی در دسترس و قابل‌استفاده بودن به‌محض تقاضای یک هستار مجاز.	۳-۱ قابلیت یک خدمت یا عنصری از خدمت برای انجام وظیفه خود در لحظه‌ای معین یا در طول دوره زمانی معنی. **یادآوری**- دسترس‌پذیری به طور معمول با نسبت مدت زمانی که خدمات واقعاً برای استفاده در دسترس بوده، به کل مدت‌زمان توافق شده خدمات تعریف می‌شود. ۳-۱۱ **یادآوری ۱**- علاوه بر آن، سایر ویژگی‌ها مانند اصالت، پاسخگویی، انکارناپذیری و قابلیت اطمینان نیز می‌تواند مطرح شود. **یادآوری ۲**- واژه «دسترس‌پذیری» در این تعریف استفاده نشده است زیرا اصطلاح تعریف‌شده‌ای در این قسمت استاندارد است و در نتیجه برای این تعریف مناسب نیست. **یادآوری ۳**- برگرفته از استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷.	به «امنیت اطلاعات» مراجعه شود. اغلب قابلیت دسترسی مرکز مدیریت خدمت در نظر گرفته می‌شود و یک نقش غالب در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در بعد ارزیابی کیفیت خدمات فراهم‌شده، ایفا می‌کند. به بند ۶-۳ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مراجعه شود. تفاوت بین دو تعریف زیاد نیست، اما به دلیل اهمیتی که بر «قابلیت دسترسی» در مدیریت خدمت قرار گرفته، تفاوت قابل توجه است. پیامد مستقیم تفاوت بین دو معنای قابلیت دسترسی این است که تعریف استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، از امنیت اطلاعات برای استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، با استفاده از دسترس‌پذیری به‌جای قابلیت دسترسی، اقتباس شده است.
تداوم کسب‌وکار	۲-۸ فرآیندها (۲-۳۱) و/یا روش‌های اجرایی (۲-۳۰) برای اطمینان از تداوم عملیات کسب‌وکار.	تعریف‌نشده	تدوام خدمت در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به‌عنوان زیرمجموعه‌ای از تداوم کسب‌وکار به‌کار می‌رود. به تداوم خدمت مراجعه شود.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
محرمانگی	۲-۹ ویژگی در دسترس یا آشکار نبودن اطلاعات برای افراد، هستارها یا فرآیندهای (۲-۳۱) غیرمجاز.	تعریف‌نشده	بدون معادل مستقیم
مبنای پیکربندی	تعریف‌نشده	۲-۳ اطلاعات پیکربندی که رسماً در نقطه‌ای از زمان در طول حیات یک خدمت یا عنصری از خدمت تعیین شده است. **یادآوری ۱**- خطوط مبنای پیکربندی به همراه تغییرات مصوب آن‌ها، اطلاعات جاری پیکربندی را تشکل می‌دهد. **یادآوری ۲**- این تعریف از استاندارد **ISO/IEC 24765:2010** آورده شده است.	این اصطلاح یک بار در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به‌کار رفته است، بند ۹-۱، در:... یک مبنای پیکربندی از CIها باید گرفته شود، پیش از آنکه یک استقرار در محیط جدید انتشار یابد.
قطعه پیکربندی	تعریف‌نشده	۳-۳ عنصری که برای ارائه خدمت یا خدمات باید تحت کنترل قرار گیرد.	CIا در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، حائز اهمیت هستند و به‌عنوان قسمتی از یک خدمت در نظر گرفته می‌شوند. CIها می‌توانند یک خدمت یا جزئی از یک خدمت باشند. یک دارایی اطلاعاتی می‌تواند یک CIباشد. به استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، تعریف ۳-۲۷ جزء خدمت مراجعه شود.
دادگان مدیریت پیکربندی	تعریف‌نشده	۴-۳ مخزن داده که برای ثبت صفات اقلام پیکربندی و ارتباط و ارتباط میان اقلام پیکربندی در طول	بر اساس رویکردی که توسط سازمان اتخاذ می‌شود، یک دادگان مدیریت پیکربندی جهت نگهداری فهرست موجودی دارایی‌ها به‌کار رود.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		چرخه حیات آن‌ها استفاده می‌شود.	به استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، پیوست الف، بند الف-۷-۱-۱ مراجعه شود.
بهبود مستمر	تعریف‌نشده	۳-۵ فعالیتی تکرارشونده برای افزایش توانمندی در جهت برآورده ساختن نیازمندی‌های خدمت. **یادآوری**- برگرفته از استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بند ۴-۱-۲، نیاز به خط‌مشی از بهبود مستمر، به‌عنوان قسمتی از خط‌مشی مدیریت خدمت دارد. چرخه PDCA، همان طور که در مقدمه استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، آمده است بسیار شبیه ISO 9001 و استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، است. برای مثال بند ۴-۲-۴ از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷ را با بند ۴-۵-۵ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مقایسه کنید.
کنترل	۲-۱۰ ابزارهای مدیریت مخاطره (۲-۳۴)، شامل خط‌مشی‌ها (۲-۲۸)، روش‌های اجرایی (۲-۳۰)، راهنماها (۲-۱۶)، اقدامات یا ساختارهای سازمانی است که می‌تواند ماهیت اداری، فنی، مدیریتی، یا حقوقی داشته باشد. ISO 31000:2009 ۲-۲۶ کنترل معیاری که مخاطره (۲-۱) را تعدیل می‌کند. **یادآوری ۱**- کنترل‌ها شامل هر فرآیند، خط‌مشی، افزاره، شیوه	تعریف‌نشده	کلمه کنترل در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، هم به‌عنوان اسم و هم به‌عنوان فعل به‌کار می‌رود اما نه به‌عنوان یک اصطلاح خاص، بنابراین معنای انگلیسی معمول اعمال می‌شود: اسم: اختیار یا اقتدار؛ قدرت تأثیرگذاری و راهنمایی، گرفتن کنترل، وسیله محدودیت. (کنترل‌ها) وسیله‌ای برای عملیات، تنظیم، یا آزمون (یک ماشین، سامانه، غیره) فعل: (کنترل‌شده، کنترل‌کردن) داشتن یا به‌کار بردن قدرت بر روی کسی یا چیزی، تنظیم کردن، محدود کردن، تنظیم یا آزمون (ماشین، سامانه، غیره)

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
	یا کنش‌های دیگر است که مخاطره را تعدیل می‌کنند. **یادآوری ۲**- کنترل‌ها ممکن است همیشه اثر تعدیل درنظرگرفته شده یا فرض شده را نشان ندهند. [ISO/IEC Guide 73:2009 , definition 3.8.1.1]		تقریباً دو کاربرد «کنترل» به‌عنوان اسم در بند ۶-۶، استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مدیریت امنیت اطلاعات، کاربردهای دیگر در بندهای ۴-۳-۲ و ۴-۴-۳ است که متن بدون تغییر از استاندارد ملی ایران شماره ۹۰۰۱، سال: ۱۳۸۸ دریافت شده است. کنترل در جاهای بسیاری به‌عنوان فعل به‌کار رفته است، معمولاً به‌عنوان: «کنترل فرآیند XXX» یا «X باید توسط Y کنترل شود.»
هدف کنترلی	۲-۱۱ بیانیه‌ای که نتیجه پیاده‌سازی کنترل‌ها (۲-۱۰) را توصیف می‌کند.	تعریف‌نشده	اسم «هدف» در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در معنای انگلیسی معمول خود به‌کار می‌رود: قصد یا آرزو به سمت چیزی، یک مقصد. رابطه باریکی بین استفاده از «هدف کنترلی» در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷ و استفاده از آن در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، وجود دارد، بندهای ۴ از عبارتی مانند «اهداف مدیریت خدمت» یا بند ۶-۶، «اهداف مدیریتی امنیت اطلاعات».
کنش اصلاحی	۲-۱۲ کنشی که برای از بین بردن علت یک عدم انطباق شناسایی‌شده یا سایر شرایط نامطلوب انجام می‌گیرد. [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.]	۶-۳ کنش برای حذف علت یا کاهش احتمال وقوع یک عدم انطباق شناخته‌شده یا سایر موقعیت‌های نامطلوب.	اصلاحات مشابهی در هر دو استاندارد استفاده می‌شود، اما تفاوت‌هایی در معانی آن‌ها وجود دارد. حذف علت همیشه ممکن یا مطلوب نیست، به‌جای آن پرهیز از تکرار می‌تواند بهتر یا مقرون به صرفه‌تر باشد. به کنش پیشگیرانه در استاندارد ملی ایران به شماره

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		یادآوری- برگرفته از استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.	۱-۱۶۳۴۷ سال:۱۳۹۱، تعریف ۳,۱۸ مراجعه شود.
مشتری	تعریف‌نشده	۳-۷ سازمان یا بخشی از سازمان که خدمت یا خدمات را دریافت می‌کند **یادآوری ۱**- مشتری می‌تواند نسبت به ارائه‌دهنده خدمت داخلی یا بیرونی باشد. **یادآوری ۲**- برگرفته از استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.	در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، یک مشتری می‌تواند به‌عنوان یک تأمین‌کننده هم عمل کند.
مستند	تعریف‌نشده	۳-۸ اطلاعات و رسانه‌ای که اطلاعات بر روی آن قرار می‌گیرد. [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.] مثال‌ها: خط‌مشی‌ها، طرح‌ها، توصیف فرآیندها، روش‌های اجرایی، تفاهم‌نامه سطح همکاری، قراردادها یا سوابق. **یادآوری ۱**- مستندسازی می‌تواند از هر نوع یا شکل رسانه استفاده کند. **یادآوری ۲- در** این مجموعه استاندارد ملی، اسناد به غیر	بدون معادل مستقیم

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		از سوابق، چیزی که باید به آن دست یافت را بیان می‌کنند.	
اثربخشی	۲-۱۳ میزانی که فعالیت‌های برنامه‌ریزی‌شده تحقق یافته و نتایج برنامه‌ریزی‌شده به‌دست آمده است. [استاندارد ملی ایران به شماره ۹۰۰۰ سال:۱۳۸۷]،	۳-۹ میزان تحقق فعالیت‌های برنامه‌ریزی‌شده و دستیابی به نتایج برنامه‌ریزی‌شده. [برگرفته از استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.]	کاملاً یکسان.
کارایی	۲-۱۴ رابطه بین نتایج حاصل‌شده و میزان مطلوبیت استفاده از منابع.	تعریف‌نشده	این کلمه در معنای انگلیسی معمول خود و فقط یک‌بار در مقدمه به‌کاررفته است. الزامی در باب کارایی نیست.
رویداد	۲-۱۵ وقوع مجموعه‌ای ویژه از شرایط ISO/IEC Guide 73:2002	تعریف‌نشده	این کلمه رویداد در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در معنای انگلیسی معمول خود به‌کار می‌رود: آنچه به وقوع می‌پیوندد یا روی می‌دهد. برای مثال، به بند ۶-۲ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مراجعه شود: «رویدادهای مهم» یا بند ۶-۳-۲: «طرح‌های تداوم خدمت و در دسترس بودن». این کاربرد مشابه استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، به طور گسترده قابل مقایسه است. به رویداد امنیت اطلاعات مراجعه شود.
راهنما	۲-۱۶ توصیه‌ای درباره آنچه انتظار می‌رود که بتوان با انجام آن به هدفی دست‌یافت.	تعریف‌نشده	به سایر قسمت‌های ISO/IEC 20000 مراجعه شود. درحالی‌که استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل نیازمندی‌های الزامی است، تمام

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			قسمت‌های دیگر ISO/IEC 20000 استانداردهای بین‌المللی اطلاعاتی یا گزارش‌های فنی هستند.
ضربه	۲-۱۷ تغییر نامطلوب در سطح تحقق اهداف کسب‌وکار.	تعریف‌نشده	کاربرد کلمه «ضربه» در هردو استاندارد به طور گسترده مشابه است. «اثر» ۲۶ بار در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در معنای انگلیسی معمول خود: اثر، اسم: اثر قوی یا تأثیر، به‌کاربرده شده است، این استفاده از «ضربه» در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، نسبت به چگونگی استفاده از آن در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، کمتر خاص است. بیشتر کاربرد در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، مربوط به مخاطره یا شرایط حقیقی منفی است. برای مثال تعریف ۳-۱۵ خطای شناخته‌شده و در بند ۵: «فراهم‌کننده خدمت باید این فرآیند را برای همه خدمات جدید و تغییرات در خدمات با پتانسیل داشتن یک تأثیر بزرگ بر روی خدمات یا مشتری، به‌کار برد.» یا بند ۶-۳-۲: «فراهم‌کننده خدمت باید تأثیر تقاضای تغییر بر روی طرح (های) تداوم خدمت و طرح (های) دسترسی را ارزیابی کند.»
رخداد	به رخدادداد امنیت اطلاعات مراجعه شود.	۳,۱۰ وقفه برنامه‌ریزی نشده یک خدمت، کاهش کیفیت	تفاوت‌های حائز اهمیتی بین استفاده از «رخداد» در مجموعه استاندارد ملی ایران به شماره ۲۷۰۰۱

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		یک خدمت یا واقعه‌ای که هنوز بر خدمت برای مشتری تأثیر شدید نگذاشته است.	سال:۱۳۸۷ و در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، وجود دارد. کلمه «رخداد» در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، به‌کار می‌رود تا به معنای «چیزی که با امنیت در محدوده محیط، اشتباه شده است» باشد. در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، کلمه «رخداد» یک معنای تعریف‌شده دارد و نسبت به استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، خاص‌تر است. در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، «رخداد» یکی از مجموعه اصطلاحات مرتبط به هم است و فقط به رخدادهای امنیت اطلاعات مربوط نمی‌شود. سایر اصطلاحات مرتبط عبارت‌اند از: ۳,۱۹ مشکل دلیل ریشه‌ای یک یا تعداد بیشتری رخداد یادآوری: دلیل اساسی معمولاً در زمان ایجاد سابقه مشکل شناخته‌شده نیست و فرآیند مدیریت خدمت مسئول بررسی بیشتر است. ۳-۱۵ خطای شناخته‌شدهشناخته‌شده مشکلی که یک دلیل ریشه‌ای شناخته‌شده یا یک روش کاهش یا حذف اثراتش بر خدمت با کار کردن حول آن، دارد.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			رخداد بزرگ (یک اصطلاح تعریف‌شده نیست) هر رخداد (مشکلی) که متعلق به بالاترین سطح طبقه اثر درنظرگرفته می‌شود. هرکدام از «رخداد»، «مشکل» و «رخداد بزرگ» به طور متفاوت مدیریت می‌شوند و موضوعی برای الزامات متفاوت هستند. «خطای شناخته‌شده» مشکلی است در جایی که دلیل اصلی شناخته‌شده و توسط فرایند مدیریت مشکل مدیریت شود، شامل الزاماتی است که هنگام وقوع مشکل شناخته‌شده به‌عنوان خطا، اعمال می‌شود. «رخداد بزرگ» توسط فرایند مدیریت رخداد و تقاضای خدمت، با الزام به اینکه یک روش اجرایی ویژه برای مدیریت «رخدادهای بزرگ» وجود دارد، مدیریت می‌شود. به رخداد امنیت اطلاعات مراجعه شود.
دارایی اطلاعاتی	۲-۱۸ دانش یا داده‌ای که برای سازمان ارزش دارد.	تعریف‌نشده	این اصطلاح یک اصطلاح تعریف‌شده نیست اما در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، استفاده شده است، برای مثال بند ۶-۶-۲: «فراهم‌کننده خدمت باید کنترل‌های امنیت فیزیکی، اداری و فنی را جهت: الف- حفظ محرمانگی، یکپارچگی و قابلیت دسترسی دارایی‌های اطلاعاتی» پیاده‌سازی و اجرا کند. به «دارایی» مراجعه شود.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
امنیت اطلاعات	۲-۱۹ حفظ محرمانگی (۲-۱۳)، یکپارچگی (۲-۳۶) و دسترس‌پذیری (۲-۱۰) اطلاعات. **یادآوری**- علاوه بر این، سایر ویژگی‌ها، همچون صحت (۲-۶)، پاسخگویی (۲-۲)، انکارناپذیری (۲-۲۷) و قابلیت اطمینان (۲-۵۶) را نیز می‌تواند در بر گیرد.	۳-۱۱ حفظ محرمانگی، یکپارچگی و دسترسی به اطلاعات **یادآوری ۱**- علاوه بر آن، سایر ویژگی‌ها مانند اصالت، پاسخگویی، انکارناپذیری و قابلیت اطمینان نیز می‌تواند مطرح شود. **یادآوری ۲**- واژه «دسترس‌پذیری» در این تعریف استفاده نشده است زیرا اصطلاح تعریف‌شده‌ای در این قسمت استاندارد است و در نتیجه برای این تعریف مناسب نیست. **یادآوری ۳**- اقتباس از استاندارد ملی ایران به شماره ۲۷۰۰۱؛ سال ۱۳۸۷.	در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، کلمه قابلیت دسترسی نمی‌تواند در تعریف امنیت اطلاعات در ۳-۱۱ به‌کاررود، زیرا قابلیت دسترسی یک اصطلاح تعریف‌شده با معنای متفاوت است (به قابلیت دسترسی مراجعه شود)؛ بنابراین تعریف برای امنیت اطلاعات اقتباس شده است تا اصطلاح دسترس‌پذیری به‌جای آن به‌کار رود. دسترس‌پذیری از تعریف قابلیت دسترسی از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، گرفته‌شده است «ویژگی در دسترس بودن و قابل‌استفاده بودن بر اساس نیاز توسط یک موجودیت مجاز».
رویداد امنیت اطلاعات	۲-۲۰ وقوع یک حالت شناسایی‌شده از سامانه، خدمت یا شبکه که به یک نقض احتمالی از امنیت اطلاعات (۲-۱۹)، خطمشی (۲-۲۸) یا شکست کنترل (۲-۱۰)، یا موقعیت ناشناخته قبلی که می‌تواند مرتبط با امنیت باشد را نشان می‌دهد.	تعریف‌نشده	رویداد امنیت اطلاعات تنها در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به‌عنوان قسمتی از تعریف ۳-۱۲: رخداد امنیت اطلاعات به‌کار رفته است. به‌علاوه، رویداد ۲-۱۵(نه رویداد امنیت اطلاعات) در: الف- تعریف مخاطره- به ۳-۲۵ مراجعه شود که شامل یادآوری ۳ و ۴ ارجاع داده‌شده به آن است که به رویدادها اشاره می‌کند. ب- تعریف تداوم خدمت (۳-۲۸) پ-استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بند ۶-۲، گزارش‌گیری خدمت

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			ت-استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بند ۶-۳-۲ طرح تداوم خدمت و قابلیت دسترسی به تعریف رویداد مراجعه شود: یک یا تعداد بیشتری رویداد می‌توانند قسمتی از رخداد امنیت را شکل دهند.
رخداد امنیت اطلاعات	۲-۲۱ یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات (۲-۲۰) ناخواسته یا پیش‌بینی‌نشده که به‌احتمال زیاد، عملیات کسب‌وکار را به خطر می‌اندازد و امنیت اطلاعات (۲-۱۹) را تهدید می‌کند.	۳-۱۲ یک یا مجموعه‌ای از وقایع (۲-۲۰) ناخواسته یا غیرمنتظره امنیت اطلاعات که با احتمال قابل‌توجهی ممکن است عملیات کسب‌وکار را به خطر اندازد و امنیت اطلاعات (۲-۱۹) را تهدید کند. [استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱]	تعریف ۳-۱۲ استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل اصطلاح رخداد امنیت اطلاعات استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، است. بند ۶-۶-۳ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل یک الزام است: مخاطرات امنیت اطلاعات باید با استفاده از روش‌های اجرایی مدیریت مخاطره مدیریت شود، با اختصاص اولویت به مخاطرات امنیت اطلاعات. این اولویت برای تهیه کردن «چیزهایی که در مورد خدمت اشتباه هستند»، وقتی علت آن یک مشکل است، نیست، به این معنا: دلیل اساسی یک یا تعداد بیشتری رخداد وقتی که دلیل اساسی معمولاً در زمان ایجاد سابقه مشکل شناخته‌شده نیست و فرآیند مدیریت خدمت مسئول بررسی بیشتر است. این مسائل با فرآیند مدیریت مشکل و نه فرآیند مدیریت رخداد و تقاضای

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			خدمت، مدیریت می‌شوند. رخدادهای [امنیت اطلاعات] بزرگ توسط فرآیند رخداد و تقاضای خدمت مرتبط با آن مدیریت می‌شوند. تنوع در راهی که اصطلاح در هر دو استاندارد استفاده می‌شود پیچیده‌تر از آن است که یک رویداد یا رخداد امنیتی زیرمجموعه یا نوع خاصی از رخداد [مدیریت خدمت] باشد. به بند ۶-۲-۵ از این استاندارد بین‌المللی مراجعه شود.
مدیریت رخداد امنیت اطلاعات	۲۲-۲ فرآیندهای (۲-۳۱) به‌منظور آشکارسازی، گزارش‌دهی، ارزشیابی، پاسخ‌دهی به رسیدگی به و یادگیری از رخدادهای امنیت اطلاعات (۲-۲۱)	تعریف‌نشده	به: «رخداد» «رخداد امنیت اطلاعات» «خطای شناخته‌شده» «مشکل» مراجعه شود.
سامانه مدیریت امنیت اطلاعات (ISMS)	۲۳-۲ قسمتی از سامانه مدیریت (۲-۲۶) کلان که مبتنی رویکرد مخاطره کسب‌وکار بوده و به‌منظور برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازبینی، نگهداری و بهبود امنیت اطلاعات (۲-۱۹)	تعریف‌نشده	به «سامانه مدیریت خدمت» و «سامانه مدیریت» مراجعه شود.
مخاطره امنیت اطلاعات	۲۴-۲ توانایی بالقوه یک تهدید (۲-۴۵)، در بهره‌جویی از آسیب‌پذیری (۲-۴۶) یک یا گروهی از دارایی‌ها (۲-	تعریف‌نشده	به «مخاطره» مراجعه شود. مخاطره امنیت اطلاعات تعریف‌نشده است اما در قسمت مدیریت امنیت اطلاعات از استاندارد ملی ایران

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
	۳) و در نتیجه آسیب زدن به سازمان.		به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بند ۶-۶-۱ به‌کاررفته‌است.
یکپارچگی	۲-۲۵ ویژگی محافظت از صحت و تمامیت دارایی‌ها (۲-۳)	تعریف‌نشده	کلمه یکپارچگی در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در معنای انگلیسی معمول خود به‌کار می‌رود: کیفیت یا حالتی که از کامل بودن بدون خرابی. (برای مثال به استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بند ۶-۶-۲ مراجعه شود: «فراهم‌کننده خدمت باید کنترل‌های امنیت فیزیکی، اداری و فنی را جهت: الف- حفظ محرمانگی، یکپارچگی و قابلیت دسترسی دارایی‌های اطلاعاتی؛ پیاده‌سازی و اجرا کند». بند ۹-۱ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل الزامات زیر است: «باید یک روش اجرایی مستند شده برای ضبط، کنترل و دنبال کردن نسخه‌های CIها وجود داشته باشد. درجه کنترل باید یکپارچگی خدمت و اجزا خدمت با توجه به الزامات خدمت و مخاطرات مرتبط با CIها، حفظ کند». «تغییرات در CIها باید قابل ردگیری و ممیزی باشد تا یکپارچگی CIها و داده‌ها در دادگان مدیریت پیکربندی را تضمین کند».

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			بند ۹-۳ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل الزامات زیر است: «انتشار باید در محیط واقعی استقرار یابد بنابراین یکپارچگی سخت‌افزار، نرم‌افزار و سایر اجزا خدمت در طول استقرار انتشار حفظ شود»
طرف ذی‌نفع	تعریف‌نشده	۳-۱۳ فرد یا گروهی که در مورد عملکرد یا موفقیت فعالیت‌های ارائه‌دهنده خدمت دارای علایق خاصی است. مثال: مشتریان، مالکین، مدیریت، افراد در سازمان ارائه‌دهنده خدمت، تأمین‌کنندگان، صاحبان بانک-ها، اتحادیه‌ها و شرکا. **یادآوری ۱**- یک گروه می‌تواند یک سازمان، بخشی از یک سازمان یا بیش از یک سازمان باشد. **یادآوری ۲**- برگرفته از استاندارد ملی ایران به شماره ۹۰۰۰؛ سال ۱۳۸۷	به «فراهم‌کننده خدمت» مراجعه شود.
گروه داخلی	تعریف‌نشده	۳-۱۴ قسمتی از سازمان ارائه‌دهنده خدمت که با ارائه-دهنده خدمت قرارداد مکتوبی تنظیم می‌کند تا در طراحی، انتقال، تحویل و بهبود یک یا چند خدمت مشارکت کند. **یادآوری**- گروه داخلی خارج از دامنه سامانه مدیریت	به «فراهم‌کننده خدمت» مراجعه شود.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		خدمات ارائه‌دهنده خدمت قرار دارد.	
خطای شناخته‌شده	تعریف‌نشده	۳-۱۵ مشکلی که علت ریشه‌ای شناخته‌شده‌ای دارد یا روش شناخته‌شده‌ای برای کاهش یا حذف تأثیر آن بر خدمت در قالب راه‌حل موقت وجود دارد.	به «رخداد» و «مشکل» مراجعه شود.
سامانه مدیریت	۲-۲۶ چارچوب خط‌مشی‌ها (۲-۲۸)، روش‌های اجرایی (۲-۳۰)، راهنماها (۲-۱۶) و منابع مرتبط به‌منظور دستیابی به اهداف سازمان.	سامانه مدیریت در یادآوری ۱ از تعریف سامانه مدیریت خدمت تعریف‌شده است: **یادآوری ۱-** سامانه مدیریتی مجموعه‌ای از عناصر مرتبط یا متعامل برای تعیین خط مشی و اهداف و دستیابی به آن اهداف است.	در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، جهت ارجاع به «سایر سامانه‌های مدیریتی» به‌کاربرده شده، استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به «سامانه مدیریت خدمت» ارجاع داده است.
انکارناپذیری	۲-۲۷ توانایی اثبات ادعای وقوع رویداد (۲-۱۵) یا کنش و هستارهای آغازکننده‌ی آن، به‌منظور حل اختلاف در مورد وقوع یا عدم وقوع رویداد (۲-۱۵) یا کنش و دخالت هستارها در رویداد (۲-۱۵)	تعریف یا استفاده‌نشده	بدون معادل مستقیم
سازمان	تعریف‌نشده	۳-۱۷ گروهی از افراد و تسهیلات با ترتیب دادن مسئولیت‌ها، اختیارات و روابط آن‌ها. مثال: شرکت، مجتمع (صنعتی، تجاری، خدماتی و غیره)، اداره، بنگاه، موسسه، بنگاه خیریه، تجارت‌خانه، انجمن یا قسمتی یا ترکیبی از آن‌ها. **یادآوری ۱-** ترتیب عموماً دارای نظم است.	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، از اصطلاح «فراهم‌کننده خدمت» و «سازمان» برای موجودیت‌های گوناگون استفاده می‌کند، بنابراین تفاوت در هر شرح برای سامانه مدیریت یکپارچه حائز اهمیت است. به «فراهم‌کننده خدمت» مراجعه شود.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		یادآوری ۲- سازمان می‌تواند عمومی یا خصوصی باشد. [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.]	
خط مشی	۲-۲۸ نیت و جهت‌گیری کلی که به طور رسمی به‌وسیله مدیریت تصریح می‌شود.	تعریف‌نشده	کلمه خط‌مشی در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در معنای انگلیسی معمول خود به‌کار می‌رود: (خط‌مشی‌ها) یک طرح اکنش، معمولاً بر اساس اصول معین، تصمیم گرفته‌شده توسط شخص یا گروه، اصل یا مجموعه‌ای از اصول که بر اساس آن تصمیم پایه‌گذاری شود، روندی از رفتار که دنبال شود. خط‌مشی‌ها در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، برای جهت‌گیری مدیریت به‌کار می‌روند. تعدادی شامل خط مشی مدیریت خدمت، توسط استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، الزام شده است. کاربرد در بین دو استاندارد به طور گسترده‌ای یکسان است.
کنش پیشگیرانه	۲-۲۹ کنشی برای از بین بردن علت یک عدم انطباق بالقوه یا سایر شرایط نامطلوب بالقوه انجام می‌گیرد. [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.]	۳-۱۸ کنشی که برای اجتناب یا حذف علت‌ها یا کاهش احتمال وقوع یک عدم انطباق بالقوه یا هر موقعیت نامطلوب بالقوه انجام می‌شود. **یادآوری**- برگرفته از استاندارد ملی ایران به شماره ۹۰۰۰:	تعاریف متفاوت است به گونه‌ای که تعریف در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بسط یافته است تا موارد زیر را شامل شود: کنش‌های اصلاحی که دلیل را از بین نمی‌برند اما به گونه‌ای بر روی آن کار می‌کنند تا از گذاشتن اثر توسط آن خودداری شود. اصطلاحات مشابهی در هر دو استاندارد استفاده می-

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		سال ۱۳۸۷.	شود، اما در معانی تفاوت‌هایی وجود دارد. در مدیریت خدمت همیشه ممکن یا مطلوب نیست که کنش‌های اصلاحی اتخاذ شود. به‌جای آن جلوگیری از تکرار می‌تواند بهتر و مقرون‌به‌صرفه تر باشد؛ بنابراین برای استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، تعریف از ISO 9000 برای مجاز شمردن این امکان، اقتباس شده است. این به کنش اصلاحی در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، تعریف ۳-۶ و استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، تعریف ۲-۱۲ ارتباط می‌دهد.
مشکل	تعریف‌نشده	۳-۱۹ علت ریشه‌ای یک یا چند رویداد. **یادآوری**- معمولاً علت ریشه‌ای مشکل هنگام ثبت آن شناخته‌شده نیست و فرآیند مدیریت مشکل مسئول بررسی-های بعدی آن است.	به «رخداد» و «خطای شناخته‌شده» مراجعه شود.
روش اجرایی/روال	۳-۲ طریقه‌ی مشخص شده‌ای برای اجرای یک فعالیت یا یک فرآیند (۲-۳۱) [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷]	۳-۲۰ راه مشخص برای انجام یک فعالیت یا یک فرآیند [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷] **یادآوری**- روش اجرایی می‌تواند مستند باشد یا نباشد.	هردو تعریف بر اساس ISO 9000 است. آنها به طور گسترده‌ای مشابه هستند. تنها یادآوری متفاوت است، بدین معنا که روال‌ها می‌توانند مستند نشوند، اما استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به همه روال‌ها به‌عنوان «روال مستند شده» ارجاع داده است. روال‌هایی که قسمتی از یک برنامه هستند

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			به‌عنوان قسمتی از یک برنامه مستند می‌شوند.
فرآیند	۳۱-۲ مجموعه فعالیت‌های مرتبط با هم یا متعامل که درونداد‌ها را به برونداد‌ها تبدیل می‌کند. [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷]	۲۱-۳ مجموعه‌ای از فعالیت‌های مرتبط و متعامل که ورودی‌ها را به خروجی‌ها تبدیل می‌کنند. [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷]	هردو بر اساس ISO 9000:2005 مشابه‌اند.
سابقه	۳۲-۲ مدرکی که در آن نتایج به‌دست آمده ذکر می‌شود یا شواهدی را دال بر انجام فعالیت فراهم می‌آورد. [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷]	۲۲-۳ سندی که نتایج به‌دست آمده را بیان می‌کند یا شواهدی را در مورد فعالیت‌های انجام‌شده، فراهم می‌کند. [استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷] **مثال**- گزارش‌های ممیزی، گزارش‌های رویداد، سوابق آموزشی یا صورت جلسات.	هردو بر اساس ISO 9000:2005 مشابه‌اند.
نسخه منتشرشده	تعریف یا استفاده‌نشده	۲۳-۳ مجموعه‌ای از یک یا چند قلم پیکربندی جدید یا تغییریافته که به‌عنوان نتیجه یک یا چند تغییر به محیط اجرا عرضه می‌شود.	بدون معادل مستقیم
قابلیت اطمینان	۳۳-۲ ویژگی سازگاری با رفتار و نتایج مورد نظر.	در ۳-۱۱ امنیت اطلاعات به آن ارجاع داده شده است: **یادآوری ۱**- علاوه بر آن، سایر ویژگی‌ها مانند اصالت، پاسخ‌گویی، انکارناپذیری و قابلیت اطمینان نیز می‌تواند	کلمه اطمینان‌پذیری در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، در معنای انگلیسی معمول خود به‌کار می‌رود: قابلیت اعتماد. به استاندارد ملی ایران به شماره ۱-۱۶۳۴۷

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		مطرح باشد.	سال:۱۳۹۱، بند ۹-۱ مراجعه شود: «دادگان مدیریت پیکربندی باید جهت تضمین اطمینان‌پذیری و درستی، مدیریت شوند، شامل کنترل دسترسی به به‌روزرسانی.»
تقاضا برای تغییر	تعریف یا استفاده‌نشده	۲۴-۳ پیشنهادی برای تغییری که باید در یک خدمت، عنصری از یک خدمت یا سامانه مدیریت خدمات اعمال شود. **یادآوری**- تغییر در یک خدمت شامل تمهید برای خدمت جدید یا حذف خدمتی که دیگر مورد نیاز نیست، می‌شود.	در پیوست الف، استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، به «مدیریت تغییر» به‌عنوان کنترل در الف-۱۰-۱-۲ اشاره شده است. بسیاری از کنترل‌ها در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، به مدیریت و کنترل تغییرات اشاره می‌کنند. برای مثال: الف-۸-۳، الف-۱۰-۲-۳، الف-۱۲-۵-۱
مخاطره	۳۴-۲ ترکیبی از احتمال وقوع یک رویداد (۲-۱۵) و پیامد آن. [ISO/IEC Guide 73:2002]	۲۵-۳ تأثیر عدم قطعیت بر روی اهداف **یادآوری ۱**- تأثیر عبارت است از انحراف مثبت یا منفی از آن چه مورد انتظار است. **یادآوری ۲**- اهداف می‌تواند جنبه‌های متفاوتی داشته باشند (مانند مالی، بهداشت و ایمنی و زیست‌محیطی) و می‌تواند در سطوح مختلفی اعمال شوند (مانند راهبردی، در سطح سازمانی، پروژه، محصول و فرآیند) **یادآوری ۳**- مخاطره اغلب با ارجاع به وقایع و پیامدهای بالقوه یا ترکیبی از آن‌ها مشخص می‌شود. **یادآوری ۴**- مخاطره اغلب برحسب ترکیبی از پیامدهای	تعداد محدودی کاربرد واضح «مخاطره» در ISO/IEC 20000 وجود دارد، هرچند بسیاری از ابعاد پیش فعالانه مدیریت خدمت دارای هدف کاهش مخاطرات هستند. بهتر است توجه شود که مفهوم «مخاطره» که در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، تحت بازبینی پذیرفته شده است، بر اساس ISO 31000 مشابه استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، است. به «آسیب‌پذیری» مراجعه شود.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		یک واقعه (شامل تغییر در محیط) و احتمال وقوع آن بیان می‌شود. [ISO 31000:2009]	
پذیرش مخاطره	۲-۳۵ تصمیم‌گیری در مورد پذیرش یک مخاطره (۲-۳۴) [ISO/IEC Guide 73:2002]	تعریف‌نشده	عبارت «پذیرش مخاطره» در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، تعریف یا استفاده نشده است. هرچند، در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، الزاماتی جهت تعریف معیاری برای پذیرش مخاطره در طرح مدیریت خدمت، بند ۴-۵-۲ و در فرآیند مدیریت امنیت اطلاعات بند ۶-۶-۱ وجود دارد. مفاهیم یکسانی در بند ۵-۴، در الزامات برای استفاده از معیار مخاطره وجود دارد.
تحلیل مخاطره	۲-۳۶ استفاده نظام‌مند از اطلاعات به‌منظور شناسایی منابع و برآورد مخاطره (۲-۳۴) [ISO/IEC Guide 73:2002] **یادآوری**- تحلیل مخاطره، پایه‌ای را برای ارزیابی مخاطره (۲-۴۱)، برطرف‌سازی مخاطره (۲-۴۳) و پذیرش مخاطره (۲-۳۵) فراهم می‌سازد.	تعریف‌نشده	به ارزیابی مخاطره مراجعه شود. توصیه می‌شود توجه ویژه‌ای اعمال شود؛ که تحلیل مخاطره به‌طورقطع «پذیرش مخاطره» نیست، برای داوری به ISO/IEC 27005 مراجعه شود.
ارزشیابی مخاطره	۲-۳۷ فرآیند (۲-۳۱) کلی تحلیل مخاطره (۲-۳۶) و ارزیابی مخاطره (۲-۴۱) [ISO/IEC Guide 73:2002]	تعریف‌نشده	ارجاعات در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به ارزیابی مخاطره مرتبط با خدمت است. برای مثال: بند ۴-۵-۳: (پیاده‌سازی و اجرای SMS) شامل «... ت- شناسایی، ارزیابی و مدیریت مخاطرات خدمات

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			می‌شود»: بند ۵-۲ (برنامه‌ریزی خدمات جدید یا تغییریافته) شامل: ج- شناسایی، ارزیابی و مدیریت مخاطرات؛ بند ۶-۶-۱: «ت- اطمینان از اینکه ارزیابی‌های مخاطره امنیت اطلاعات در بازه‌های زمانی تعیین‌شده اجرا می‌شوند»؛
اطلاع‌رسانی مخاطره	۲-۳۸ تبادل یا به اشتراک‌گذاری اطلاعات درباره مخاطره (۲-۳۴) بین تصمیم‌گیرنده و سایر ذی‌نفعان [ISO/IEC Guide 73:2002]	تعریف‌نشده	در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به طریقی که مرتبط با مخاطره باشد استفاده نمی‌شود.
معیار مخاطره	۲-۳۹ شرایط مرجع که اهمیت مخاطره (۲-۳۴) بر اساس آن‌ها ارزشیابی می‌شود. [ISO/IEC Guide 73:2002]	تعریف‌نشده	در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، به شیوه مشابهی همراه با کاربرد آن در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، مورد استفاده قرار گرفته است، برای مثال: در بند ۴-۵-۲ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱،
برآورد مخاطره	۲-۴۰ فعالیت تخصیص دادن مقدار به احتمال وقوع و پیامدهای مخاطره (۲-۳۴) [ISO/IEC Guide 73:2002]	تعریف‌نشده	به «ارزیابی مخاطره» مراجعه شود.
ارزیابی مخاطره	۲-۴۱ فرآیند (۲-۳۱) مقایسه مخاطره (۲-۳۴) برآورد شده با معیار مخاطره (۲-۳۹) مفروض به‌منظور تعیین	تعریف‌نشده	به «ارزیابی مخاطره» مراجعه شود.

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
	اهمیت مخاطره (۲-۳۴) [ISO/IEC Guide 73:2002]		
عنصر خدمت	تعریف‌نشده	۳-۲۷ یک واحد از خدمت که پس از این که با سایر واحدها ترکیب شد خدمت کاملی را عرضه می‌کند. مثال‌ها: سخت‌افزار، نرم‌افزار، ابزار، برنامه‌های کاربردی، مستندات، اطلاعات، فرآیندها یا خدمات پشتیبانی **یادآوری**- یک عنصر خدمت می‌تواند از یک یا چند قلم پیکربندی تشکیل شود.	بدون معادل مستقیم
تداوم خدمت	تعریف‌نشده	۳-۲۸ توانایی مدیریت مخاطرات و وقایعی که می‌توانند تأثیرات جدی بر یک یا چند خدمت داشته باشند، به‌منظور ارائه مداوم خدمت در سطح توافق شده.	به «آسیب‌پذیری» و «مخاطرات» مراجعه شود. به «تداوم کسب‌وکار» مراجعه شود. تداوم خدمت به طور معمول به‌عنوان زیرمجموعه‌ی تداوم کسب‌وکار درنظرگرفته می‌شود.
توافق‌نامه سطح خدمت	تعریف‌نشده	۳-۲۹ توافق‌نامه مستند بین یک ارائه‌دهنده خدمت و مشتری است که خدمت و سطح توافق‌شده خدمت را شناسایی می‌کند. **یادآوری ۱**- توافقنامه سطح همکاری می‌تواند بین ارائه-دهنده خدمت و تأمین‌کننده، گروه داخلی یا مشتری که نقش تأمین‌کننده را بازی می‌کند منعقد شود. **یادآوری ۲- توافقنامه** سطح خدمت می‌تواند در قرارداد یا	این اصطلاح در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، به‌کار نرفته است. هرچند، این مفهوم در ارتباط با اهداف کنترلی در نظر گرفته‌شده در الف-۱۰-۲، وقتی ابعاد امنیت خدمت که توسط طرف سوم تحویل و نگهداری می‌شوند، اقتباس شده است. برای مثال کنترل الف-۱۰-۲-۱ (سطوح تداوم خدمت توافق شده)

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		هر نوع دیگری از توافق‌نامه‌ی مستند شده، گنجانده شود.	
مدیریت خدمت	تعریف‌نشده	۳-۳۰ مجموعه‌ای از قابلیت‌ها و فرآیندها برای هدایت و کنترل فعالیت‌ها و منابع ارائه‌دهنده خدمت در زمینه طراحی، انتقال، تحویل و بهبود خدماتی که الزامات خدمت را برآورده می‌سازد.	اهداف کنترلی در الف-۱۰-۲ از استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، به این اصطلاح مربوط است.
سامانه مدیریت خدمات (SMS)	تعریف‌نشده	۳-۳۱ سامانه مدیریت برای هدایت و کنترل فعالیت‌های مدیریت خدمات ارائه‌دهنده خدمت. **یادآوری ۱**- یک سامانه مدیریت مجموعه‌ای از عناصر مرتبط و متعامل برای تعیین خط‌مشی و اهداف و دستیابی به آن اهداف است. **یادآوری ۲**- سامانه مدیریت خدمات شامل همه خط‌مشی-ها، اهداف، طرح‌ها، فرآیندها، مستندات و منابع لازم مدیریت خدمات برای طراحی، انتقال، تحویل و بهبود خدمت و برآورده ساختن الزامات این استاندارد است. **یادآوری ۳**- برگرفته از تعریف «سامانه مدیریت کیفیت» در استاندارد ملی ایران به شماره ۹۰۰۰: سال ۱۳۸۷.	به «سامانه مدیریت امنیت اطلاعات (ISMS)» مراجعه شود.
تأمین‌کننده	تعریف‌نشده	۳-۳۵ سازمان یا قسمتی از سازمان که نسبت به سازمان ارائه‌دهنده خدمت، بیرونی محسوب شده و	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، شامل ارجاعاتی به و الزاماتی برای مدیریت موارد زیر است:

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
		قراردادی را با ارائه‌دهنده خدمت منعقد می‌سازد تا در طراحی، انتقال، تحویل و بهبود خدمت یا خدمات یا فرآیندها مشارکت کند. **یادآوری**- تأمین‌کننده شامل پیمانکاران فرعی این تأمین‌کنندگان اصلی نمی‌شود.	آ- تأمین‌کنندگان ب- تأمین‌کنندگان اصلی (کسانی که تأمین‌کنندگان فرعی را مدیریت می‌کنند) پ- گروه‌های داخلی (همکاری در ارائه خدمت) ت- مشتریان (وقتی به‌عنوان تأمین‌کننده عمل می‌کنند). همه در ارائه خدمت کلی همکاری می‌کنند و توسط فراهم‌کننده خدمت مدیریت می‌شوند: مدیریت تأمین‌کننده، تأمین‌کنندگان/تأمین‌کنندگان اصلی (و به‌واسطه تأمین‌کنندگان اصلی، تأمین‌کنندگان فرعی) را پوشش می‌دهد. مدیریت سطح خدمت مدیریت گروه‌های داخلی و مشتریان را، وقتی که به‌عنوان تأمین‌کننده عمل می‌کنند، پوشش می‌دهد. استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، از اصطلاح «تأمین‌کننده» تنها یک‌بار استفاده کرده است.
بیانیه کاربست پذیری	۴۴-۲ بیانیه مستندی که اهداف کنترلی (۲-۱۱) و کنترل‌های (۲-۱۰) مرتبط و کاربردپذیر در ISMS(۲-۲۳) سازمان را تشریح می‌کند.	تعریف یا استفاده‌نشده	در بند ۱-۲ از استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، عبارت کاربرد مشابه کاربست‌پذیری در استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، نیست.
تهدید	۴۵-۲ عامل بالقوه رخدادی ناخواسته که ممکن است باعث آسیب‌رسانی به سامانه یا سازمان شود.	تعریف‌نشده	در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، عبارت «تهدید» یک‌بار در تعریف ۳-۱۲ به‌کاررفته است:

اصطلاح	استاندارد ملی ایران به شماره ۲۷۰۰۰ سال:۱۳۹۱	استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱	توضیحات کاربرد اصطلاح در هر دو استاندارد
			«رخداد امنیت اطلاعات: یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات ناخواسته یا غیرمنتظره که دارای احتمال بالایی از به خطر افتادن عملیات کسب‌وکار و تهدید امنیت اطلاعات باشد.»
انتقال	تعریف‌نشده	۳-۳۷ فعالیت‌های درگیر در انتقال یک خدمت جدید یا تغییریافته به/از محیط واقعی	همان طور که در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، بند ۵ به‌کاربرده شده است، یک پیوند که بین گذار وجود دارد و روشی که در آن با توجه به استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، برخی تغییرات کنترل می‌شوند. همچنین فرآیندهای کنترل که در بندهای ۵ و ۹ در استاندارد ملی ایران به شماره ۱-۱۶۳۴۷ سال:۱۳۹۱، توصیف شده‌اند، خیلی به این مفهوم مرتبط هستند. استاندارد ملی ایران به شماره ۲۷۰۰۱ سال:۱۳۸۷، مدیریت تغییر را در بندهای زیر به‌کاربرده است: الف-۱۰-۱-۲ مدیریت تغییر روال‌های عملیاتی و مسئولیت‌ها الف-۱۰-۲-۳ مدیریت تغییرات برای خدمات طرف سوم
آسیب‌پذیری	۲-۴۶ ضعف یک دارایی (۲-۳) یا کنترل (۲-۱۰) که می‌تواند توسط تهدید (۲-۴۵)، مورد بهره‌جویی قرار گیرد.	تعریف یا استفاده‌نشده	بدون معادل مستقیم

کتاب‌نامه

[1] ISO 9000, Quality management systems — Fundamentals and vocabulary
[2] ISO 9004, Quality management systems — Guidelines for performance improvements
[3] ISO/IEC TS 15504-8, Information technology — Service management — Part 8: Process assessment mode for service management (under development)
[4] ISO 19011, Quality management systems — Guidelines for quality and/or environmental management systems auditing
[5] ISO/IEC 20000-2, Information technology — Service management — Part 2: Guidance on the application of service management systems
[6] ISO/IEC 20000-3, Information technology — Service management — Part 3: Guidance on scope definition and applicability for ISO/IEC 20000-1
[7] ISO/IEC TR 20000-4, Information technology — Service management — Part 4: Process reference model for service management
[8] ISO/IEC TR 20000-5, Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1
[9] ISO/IEC TR 90006, Information technology — Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011
[10] ISO/IEC 27002, Information technology — Security techniques — Information security management systems — Code of practice for information security controls (under revision)
[11] ISO/IEC 27003, Information technology — Security techniques — Information security management systems — Information security management system implementation guidance
[12] ISO/IEC 27004, Information technology — Security techniques — Information security management systems — Information security management measurements
[13] ISO/IEC 27005, Information technology — Security techniques — Information security management systems — Information security risk management
[14] ISO/IEC 27006, Information technology — Security techniques — Information security management systems — Requirements for bodies providing audit and certification of information security management systems
[15] ISO/IEC 27007, Information technology — Security techniques — Information security management systems — Guidelines for information security management systems auditing
[16] ISO/IEC TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls
[17] ISO/IEC 27010, Information technology — Security techniques — Information security management systems — Information security management for inter-sector and inter-organizational communications
[18] ISO/IEC 27014, Information technology — Security techniques — Information security management systems — Governance of information security
[19] ISO 31000, Risk management — Principles and Guidelines on Implementation