INSO- ISO-IEC

27013
1st. Revision
2017

Identical with
ISO/IEC
27013:2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
ایزو- آی ایی سی
۲۷۰۱۳
تجدید نظر اول
۱۳۹۶

فناوری اطلاعات- فنون امنیتی- راهنمای پیاده‌سازی یکپارچهٔ 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, 03.100.70, 35.030

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri .gov.ir

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی 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 واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

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

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه 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 بین‌المللی یکاها، 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

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

«تجدیدنظر اول»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات- سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون مدیر کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
عباسپور، مقصود (دکتری مهندسی کامپیوتر- معماری)	دانشیار– معاون مرکز فناوری دانشگاه شهید بهشتی
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکتری مهندسی کامپیوتر)	دانشیار- دانشگاه شهید بهشتی

اعضاء: (اسامی به ترتیب حروف الفبا)	**سمت و/ یا محل اشتغال:**
نصیری آسایش، حمیدرضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی
ویراستار:	**سمت و/ یا محل اشتغال:**
معروف، سینا (لیسانس مهندسی کامپیوتر- سخت‌افزار)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار ح
مقدمه ط
۱ هدف و دامنه کاربرد ۱
۲ مراجع الزامی ۱
۳ اصطلاحات، تعاریف و کوته‌نوشت‌ها ۲
۴ مرورکلی استانداردهای ISO/IEC 27001 و ISO/IEC20000-1 ۲
۴-۱ درک استانداردها ۲
۴-۲ مفاهیم ISO/IEC 27001 ۳
۴-۳ مفاهیم ISO/IEC20000-1 ۳
۴-۴ شباهت‌ها و تفاوت‌ها ۳
۵ رویکردها برای پیاده‌سازی یکپارچه ۶
۵-۱ کلیات ۶
۵-۲ ملاحظات دامنه کاربرد ۷
۵-۳ فرانامه‌های(سناریوهای) پیش از پیاده‌سازی ۸
۵-۳-۱ کلیات ۸
۵-۳-۲ هیچ استانداری به عنوان پایه‌ای برای سامانه مدیریت استفاده نشده است ۸
۵-۳-۴ سامانه‌های (مدیریت)ی جدا وجود دارند که الزامات هر یک از استانداردها را برآورده می‌کند ۱۰
۶ ملاحظات یکپارچهٔ پیاده‌سازی ۱۱
۶-۱ کلیات ۱۱
۶-۲ چالش‌های بالقوه ۱۲
۶-۲-۱ کاربرد و معنای دارایی ۱۲
۶-۲-۲ طراحی و انتقال خدمات ۱۳
۶-۲-۳ ارزیابی و مدیریت مخاطره ۱۳
۶-۲-۴ تفاوت‌ها در سطوح پذیرش مخاطرات ۱۵
۶-۲-۵ مدیریت رخداد و مسائل ۱۵
۶-۲-۶ مدیریت تغییر ۱۹
۶-۳ بهره بالقوه ۱۹
۶-۳-۱ استفاده از چرخه‌ی طرح-انجام-بازبینی-اقدام ۱۹
۶-۳-۲ مدیریت و گزارش سطح خدمات ۱۹

عنوان **صفحه**

۶-۳-۳ تعهدات مدیریت ۲۰
۶-۳-۴ مدیریت ظرفیت ۲۱
۶-۳-۵ مدیریت مخاطره‌ی طرف سوم ۲۱
۶-۳-۶ مدیریت تداوم و در دسترس بودن ۲۲
۶-۳-۷ مدیریت تامین کننده ۲۳
۶-۳-۸ مدیریت پیکربندی ۲۳
۶-۳-۹ مدیریت انتشار و استقرار ۲۴
پیوست الف (آگاهی‌دهنده) مطابقت بین استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 ۲۵
پیوست ب (آگاهی‌دهنده) مقایسه اصطلاحات استانداردهای ISO/IEC 27000 و ISO/IEC 20000-1 ۳۲
کتاب‌نامه ۵۵

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- راهنمای پیاده‌سازی یکپارچهٔ استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1» که نخستین بار در سال ۱۳۹۳ بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شمارهٔ ۵ تدوین و منتشر شد، بر اساس پیشنهادهای دریافتی و بررسی و تایید کمیسیون‌های مربوط برای اولین بار مورد تجدیدنظر قرار گرفت و در چهارصد و نود و هفتمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۶/۰۲/۱۷ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در بافت صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت؛ بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره ۲۷۰۱۳: سال ۱۳۹۳ است.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 27013: 2015, Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

مقدمه

رابطه بین مدیریت امنیت اطلاعات و مدیریت خدمت چنان نزدیک است که بسیاری از سازمان‌ها منافعِ پذیرش این دو استاندارد: استاندارد ISO/IEC 27001 برای مدیریت امنیت اطلاعات و استاندارد ISO/IEC 20000-1 برای مدیریت خدمت، را برای این حوزه‌ها تشخیص می‌دهند. برای هر سازمان، بهبود مسیرِ بهره-برداری برای دستیابی به انطباق با الزامات مشخص شده در یکی از این دو استاندارد و سپس ایجاد بهبودهای بیشتر برای دستیابی به انطباق با الزاماتِ استاندارد دیگر، امری متداول است.

مزایای متعددی در پیاده‌سازی سامانهٔ یکپارچه مدیریت وجود دارد که نه تنها خدمات فراهم شده بلکه همچنین حفاظت اطلاعات را در نظر می‌گیرد. این مزایا می‌توانند کسب شوند؛ چه زمانی که یک استاندارد قبل از دیگری پیاده‌سازی شود و چه زمانی که هر دو استاندارد به‌صورت هم‌زمان پیاده‌سازی شوند. به ویژه، فرایندهای مدیریتی و سازمانی می‌توانند از مفاهیم و شباهت‌های تقویت‌کنندهٔ متقابل بین این دو استاندارد و از اهداف مشترکِ آن‌ها، بهره‌مند شوند.

مزایای کلیدی پیاده‌سازی یکپارچهٔ مدیریت امنیت اطلاعات و مدیریت خدمت شامل موارد زیر است:

الف- اعتبار برای مشتریان درونی یا بیرونی سازمان در خدمت موثر و امن؛

ب- هزینه پایین‌تر برنامه یکپارچه برای دو پروژه، در مواقعی که مدیریت موثر و کارای خدمات و امنیت اطلاعات، قسمتی از راهبرد سازمان هستند؛

پ- کاهش زمان پیاده‌سازی به دلیل توسعهٔ یکپارچه فرایندهایی که برای هر دو استاندارد مشترک هستند؛

ت- ارتباطات بهتر، کاهش هزینه و کارایی عملیاتی بهبودیافته از طریق حذف دوباره‌کاری‌های غیرضروری؛

ث- درک بیشتر کارکنان مدیریت خدمت و امنیت از دیدگاه‌های یکدیگر؛

ج- سازمانِ دارای گواهینامه استاندارد ISO/IEC 27001 می‌تواند به آسانی الزامات امنیت اطلاعات را که در استاندارد ISO/IEC 20000-1:2011 بند ۶-۶ مشخص شده است، برآورده کند، چراکه هر دو استاندارد از نظر الزامات مکمل یکدیگر هستند.

در این استاندارد، راهنمایی بر مبنای نسخه‌های منتشر شده از استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 است.

این استاندارد مورد استفادهٔ افرادی است که نسبت به هر دو استاندارد، یکی از استانداردها یا هیچ کدام از استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1، آگاهی دارند.

انتظار می‌رود تا تمامی خوانندگان به رونوشت‌های هر دو استاندارد ISO/IEC 27001 و ISO/IEC 20000-1 دسترسی داشته باشند. در نتیجه، این استاندارد هیچ کدام از قسمت‌های این دو استاندارد را بازتولید

نمی‌کند. به همین ترتیب، تمام قسمت‌های استانداردها را به‌صورت کامل توصیف نمی‌کند. تنها آن قسمت‌هایی توصیف شده‌اند که موضوع مورد نظر دارای هم‌پوشانی باشند.

این استاندارد راهنماییِ مرتبط با قانون[1] و مقررات خارج از واپایش (کنترل) [2] سازمان را فراهم نمی‌کند. این موارد امکان دارد در هر کشوری متفاوت باشند و در طرح‌ریزی سامانهٔ مدیریت سازمان تاثیر داشته باشد.

1 - Legislation
2 - Control

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

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و ارائه راهنما برای پیاده‌سازی یکپارچه استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 برای سازمان‌هایی است که قصد انجام یکی از موارد زیر را دارند:

الف- پیاده‌سازی استاندارد ISO/IEC 27001، زمانی که استاندارد ISO/IEC 20000-1 قبلا پیاده‌سازی شده یا برعکس،

ب- پیاده‌سازی استانداردهای ISO/EC 27001 و ISO/IEC 20000-1 با همدیگر یا

پ- یکپارچه‌سازیِ سامانه‌های مدیریت موجود بر مبنای استانداردهای ISO/IEC27001 و ISO/IEC 20000-1.

این استاندارد تنها بر پیاده‌سازی یکپارچهٔ سامانهٔ مدیریت امنیت اطلاعات (ISMS) که در استاندارد ISO/IEC 27001 مشخص شده و سامانهٔ مدیریت خدمت (SMS) که در استاندارد ISO/IEC20000-1 مشخص شده است، تمرکز دارد.
در عمل، استانداردهای ISO/IEC 27001 و ISO/IEC20000-1 می‌توانند با دیگر استانداردهای سامانه مدیریت مانند استانداردهای ISO 9001 و ISO 14001 ادغام شوند.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به‌صورت الزامی به آن‌ها ارجاع داده شده است. بدین ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

درصورتی‌که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ایزو- آی ای سی ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی - سامانه‌های (سیستم‌های) مدیریت امنیت اطلاعات مرور کلی و واژگان

۲-۲ استاندارد ملی ایران شماره ایزو- آی ای سی ۲۷۰۰۱: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی - سامانه (سیستم) مدیریت امنیت اطلاعات- الزامات

2-3 ISO/IEC 20000-1:2011, Information technology — Service management — Part 1: Service management system requirements

2-4 ISO/IEC/TR 20000-10, Information technology — Service management — Part 10: Concepts and terminology

۳ اصطلاحات، تعاریف و کوته‌نوشت‌ها

در این استاندارد، اصطلاحات و تعاریف تعیین‌شده در استانداردهای ISO/IEC 27000، ISO/IEC 20000-1 و گزارش فنی ISO/IEC/TR 20000-10، به‌کار می‌رود.

در این استاندارد، کوته‌نوشت‌های زیر به‌کار می‌رود:

سامانه مدیریت امنیت اطلاعات (از استاندارد ISO/IEC 27001)	Information Security Management System	ISMS
سامانه مدیریت خدمت (از استاندارد ISO/IEC 20000-1)	Service Management System	SMS

پیوست الف مقایسه‌ای از محتوا در سطحِ بند، بین استانداردهای ISO/IEC 27001 و ISO/IEC20000-1 ارائه می‌کند.

پیوست ب مقایسه‌ای از اصطلاحات تعریف شده زیر ارائه می‌کند:

- استاندارد ISO/IEC 27000، واژه‌نامه برای استاندارد ISO/IEC 27001؛
- اصطلاحات استفاده شده در استاندارد ISO/IEC27001؛
- اصطلاحات تعریف شده یا استفاده‌شده در استاندارد ISO/IEC 20000-1 یا ISO/IEC/TR 20000-10.

۴ مرور کلی استانداردهای ISO/IEC 27001 و ISO/IEC20000-1

۴-۱ درک استانداردها

پیش از طرح‌ریزی سامانه یکپارچهٔ مدیریت برای مدیریت امنیت اطلاعات و مدیریت خدمت، بهتر است سازمان درکی خوب از مشخصه‌ها، شباهت‌ها و تفاوت‌های استاندارد ISO/IEC27001 و ISO/IEC20000-1 داشته باشد. این امر زمان و منابع دردسترس برای پیاده‌سازی را بیشینه می‌کند. بندهای ۴-۲ تا ۴-۴ مقدمه‌ای از مفاهیم اصلی را در هر دو استاندارد ارائه می‌کند، اما توصیه نمی‌شود به‌عنوان جایگزین برای

بازنگریِ تفصیلی استفاده شود.

۴-۲ مفاهیم استاندارد ISO/IEC 27001

استاندارد ISO/IEC 27001 مدلی برای برقراری، پیاده‌سازی، نگهداشت و بهبود مستمر ISMS به منظور محافظت از اطلاعات فراهم می‌کند. اطلاعات می‌تواند هر شکلی به خود بگیرد، در هر شکلی ذخیره شود و برای هر هدفی توسط سازمان یا درون آن استفاده شود.

به منظور دستیابی به انطباق با الزامات مشخص شده در استاندارد ISO/IEC 27001، توصیه می‌شود سازمان ISMS مبتنی بر فرایند ارزیابی مخاطره[1] برای شناسایی مخاطرات اطلاعاتی پیاده‌سازی نماید. به عنوان قسمتی از این کار، توصیه می‌شود سازمان اقدامات مختلفی را انتخاب، پیاده‌سازی، پایش و بازبینی کند تا این مخاطرات را مدیریت نماید. این اقدامات به عنوان واپایش شناخته می‌شوند. توصیه می‌شود سازمان سطوح قابل قبول مخاطره را تعیین کند، الزامات قسمت‌های مربوط به امنیت اطلاعات را در نظر بگیرد. مثال‌هایی از این الزامات عبارت‌اند از الزامات کسب‌وکار، الزامات قانونی و مقرراتی یا تعهدات قراردادی.

استاندارد ISO/IEC 27001 می‌تواند توسط هر نوع سازمان و با اندازه‌های مختلف استفاده شود.

۴-۳ مفاهیم استاندارد ISO/IEC 20000-1

استاندارد ISO/IEC 20000-1 می‌تواند توسط هر سازمان یا قسمت‌هایی از سازمان که خدماتی را استفاده یا فراهم می‌کند، استفاده شود. این امر برای مشتری و فراهم‌ساز خدمت ارزش‌افزوده دارد. توصیه می‌شود تمامی فرایندهای پوشش داده توسط این استاندارد توسط فراهم‌ساز خدمت واپایش شود، حتی اگر بعضی از فرایندها توسط قسمت‌های دیگر بهره‌برداری شوند. تنها فراهم‌ساز خدمت است که با الزامات مشخص شده در استاندارد ISO/IEC 20000-1 انطباق دارد.

سامانه SMS فعالیت‌ها و منابعِ فراهم‌ساز خدمت در طراحی، توسعه و انتقال، عملیات و بهبود خدمات را هدایت و واپایش می‌کند تا الزامات خدمت را به‌صورت پذیرفته شده توسط مشتری(ان) خود برآورده نماید.

برای برآورده نمودن الزامات مشخص شده در استاندارد ISO/IEC 20000-1، توصیه می‌شود فراهم‌ساز خدمت محدوده‌ای از فرایندهای مدیریت خدمت را پیاده‌سازی نماید. این محدوده شامل مدیریت رخداد، مدیریت تغییرات و مدیریت مساله[2] و نمونه‌هایی از این دست، می‌شود. مدیریت امنیت اطلاعات یکی از فرایندهای مدیریت خدمت در استاندارد ISO/IEC 20000-1 است.

استاندارد ISO/IEC 20000-1 می‌تواند توسط هر نوع سازمان، با هر اندازه‌ای، استفاده شود.

۴-۴ شباهت‌ها و تفاوت‌ها

مدیریت خدمت و مدیریت امنیت اطلاعات اغلب به گونه‌ای تلقی می‌شوند که گویی نه با یکدیگر ارتباط دارند

1 - Risk assessment
2 - Problem management

و نه وابستگی. بافت چنین تفکیکی به این دلیل است که مدیریت خدمت می‌تواند به راحتی با کارایی و سودآوری مرتبط باشد، در حالی که مدیریت امنیت اطلاعات اغلب به‌صورت بنیادی برای تحویل موثر خدمات درنظر گرفته نمی‌شود. در نتیجه، در ابتدا، مدیریت خدمت به‌صورت مکرر پیاده‌سازی می‌شود؛ اما همان‌طور که در شکل ۱ نشان داده شده است، بسیاری از اهداف واپایشی و واپایش‌هایِ پیوست الف در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، در الزامات مدیریت خدمت برای SMS مشخص شده در استاندارد ISO/IEC 20000-1 شامل می‌شود.

شکل ۱- مقایسهٔ بین مفاهیم استانداردهای ISO/IEC 27001 و ISO/IEC 200001-1

مدیریت امنیت اطلاعات و مدیریت خدمت به وضوح به فرایندها و فعالیت‌های مشابه بسیاری می‌پردازد، اگر چه هر سامانهٔ مدیریت، جزئیاتی متفاوت از خود نشان می‌دهد. برای اطلاعات بیشتر به پیوست الف مراجعه شود. هنگام کار با دو استاندارد، توصیه می‌شود درک شود که مشخصه‌های این دو استاندارد در بیش از یک

مورد با یکدیگر تفاوت دارند. به طور مثال، تفاوت در هدف و دامنه کاربرد (به بند ۵-۲ مراجعه شود). آن‌ها همچنین دارای اهداف متفاوتی هستند. استاندارد ISO/IEC 20000-1 برای حصول اطمینان از این که سازمان خدماتی موثر را فراهم می‌کند طراحی شده، در حالی که استاندارد ISO/IEC 20000-1 برای توانا ساختن سازمان برای مدیریت مخاطرات امنیت اطلاعات و پیشگیری از رخدادهای امنیتی به‌کار گرفته شده است.

۵ رویکردها برای پیاده‌سازی یکپارچه

۵-۱ کلیات

سازمانی که طرح‌ریزی کرده است برای پیاده‌سازی استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 می‌تواند یکی از سه حالت زیر را به خود گیرد:

- ترتیباتِ[1] نیازمحور[2] مدیریتی وجود دارد که مدیریت امنیت اطلاعات و مدیریت خدمت را پوشش می‌دهد (سامانه‌های رسمی مدیریت می‌تواند برای هر حوزه دیگر مانند مدیریت کیفیت نیز به‌کار رود)؛
- سامانه مدیریت وجود دارد که مبتنی بر این دو استاندارد است.
- سامانه‌های مدیریت جداگانه‌ای مبتنی بر این دو استاندارد وجود دارد اما یکپارچه نیستند.

توصیه می‌شود طرح‌ریزی سازمان برای پیاده‌سازی سامانه یکپارچه مدیریت برای امنیت اطلاعات و مدیریت خدمت کمینه به‌صورت زیر در نظر گرفته شود:

الف- دیگر سامانه(های) مدیریتی از قبل در حال استفاده‌اند (به طور مثال، سامانهٔ مدیریت کیفیت)؛

ب- تمامی خدمات، فرایندها و دیگر وابستگی‌ها در بافت سامانه یکپارچه مدیریت؛

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

ت- عناصری که باید به‌صورت جداگانه باقی بمانند؛

ث- تاثیر سامانهٔ مدیریت یکپارچه بر مشتریان، منابع و طرف‌های دیگر؛

ج- تاثیر رویِ فناوریِ مورد استفاده؛

چ- تاثیر بر، یا مخاطره در خدمات و مدیریت خدمت؛

ح- تاثیر بر، یا مخاطره بر امنیت اطلاعات و مدیریت امینت اطلاعات؛

خ- آموزش و یادگیری در سامانهٔ یکپارچه مدیریت؛

1 - Arrangements
2 - Ad-hoc

د- مراحل و دنبالهٔ فعالیت‌های پیاده‌سازی؛

۲-۵ ملاحظات دامنه کاربرد

یکی از ناحیه‌هایی که دو استاندارد به‌صورت چشم‌گیری با یکدیگر تفاوت دارند، در موضوع دامنه است، یعنی این‌که بهتر است سامانهٔ مدیریت چه دارایی‌ها، فرایندها و قسمت‌هایی از سازمان را شامل شود.

استاندارد ISO/IEC 20000-1 به طراحی، انتقال، تحویل و بهبود خدمات برای تحویل ارزشِ کسب‌وکار مربوط است. این موضوع با تعریف الزامات خدمت برای تحویل اهداف و سپس هماهنگ کردن خط‌مشی‌ها، فرایندها، طرح‌ها و منابع به منظور توسعه مدیریت و بهبود این خدمات کسب می‌شود. دامنه کاربرد استاندارد ISO/IEC 20000-1 شامل اهداف، خط‌مشی‌ها، طرح‌ها، فرایندها و منابع و بعلاوه خدمات می‌شود.

استاندارد ISO/IEC 27001 با چگونگی مدیریت مخاطره‌ی امنیت اطلاعات سروکار دارد. دامنه کاربرد استاندارد ISO/IEC 27001 آن قسمت‌هایی از فعالیت‌هایش که سازمان تمایل به حفظ امنیت آن‌ها را دارد پوشش می‌دهد. در نتیجه، پیاده‌سازی استاندارد ISO/IEC 27001 برای همان دامنه کاربرد به‌صورت استاندارد ISO/IEC 20000-1 ممکن است اما استاندارد ISO/IEC 20000-1 نمی‌تواند برای تمامی سازمان‌ها به‌کار گرفته شود مگر اینکه این سازمان به‌صورت کامل فراهم‌کننده خدمت باشد.

لذا، فرایندها، دارایی‌ها و نقش‌های قطعی در سازمان ممکن است از دامنه کاربرد برای ISMS توسعه‌یافته برای دستیابی به انطباق با الزامات استاندارد ISO/IEC 27001 مستثنا شود. برای استاندارد ISO/IEC 20000-1 اگر آن‌ها قسمتی از خدمات دامنه کاربرد SMS باشند، ممکن است از دامنه کاربرد مستثنا نشوند. دامنه کاربرد ISMS ممکن است به‌صورت انحصاری توسط مرز فیزیکی واضحی مانند محیط امنیتی تعریف شده باشد.

در بعضی موارد، الزامات کلی دو استاندارد نمی‌تواند برای همه یا حتی قسمتی از فعالیت‌های سازمان پیاده‌سازی شود. به‌عنوان‌مثال وقتی سازمانی قادر نیست با الزامات مشخص شده در استاندارد ISO/IEC 20000-1 انطباق یابد به این دلیل که دارای نظارت تمامی فرایندها عمل شده توسط قسمت‌های دیگر نیست.

سازمان می‌تواند SMS و ISMS را با همپوشانی بین دامنه‌های کاربرد متفاوت پیاده‌سازی نماید. در موقعیتی که اقدامات درون دامنه کاربرد استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 قرار می‌گیرد، توصیه می‌شود سامانهٔ یکپارچه مدیریت هردو استاندارد را در نظر بگیرد (به پیوست الف مراجعه شود). تفاوت‌ها در دامنه کاربرد می‌تواند سبب شود که بعضی از خدمات مشمول در SMS در ISMS موجود نباشند. به طور برابر، SMS می‌تواند از فرایندها و کارکردهای ISMS مستثنا باشد. به طور مثال، بعضی سازمان‌ها پیاده‌سازی کردن ISMS را تنها در عملیات و کارکردهای ارتباطی خود انتخاب می‌کنند، در حالی که خدمات مدیریت کاربردی در SMS آن‌ها وجود دارد. به صورت دوره‌ای، ISMS می‌تواند تمامی خدمات را پوشش دهد، در حالی که SMS می‌تواند تنها خدماتی را برای مشتری ویژه یا بعضی از خدمات را برای تمامی مشتری‌ها

پوشش دهد. توصیه می‌شود سازمان دامنه‌های کاربرد سامانه‌های مدیریت را تا جای ممکن به منظور کسب اطمینان از یکپارچگی موفق تنظیم کند.

یادآوری- راهنمایی دربارهٔ تعریف دامنه کاربرد برای استاندارد ISO/IEC 20000-1 در استاندارد ISO/IEC 20000-3 موجود است. راهنمایی برای تعریف دامنه کاربرد استاندارد ISO/IEC 27001 در استاندارد ISO/IEC 27003 در دسترس است.

۵-۳ فرانامه‌های(سناریوهای) [1] پیش از پیاده‌سازی

۵-۳-۱ کلیات

سازمانی که برای سامانه یکپارچه مدیریت طرح‌ریزی کرده است، می‌تواند یکی از سه حالت را داشته باشد، همان‌طور که در بندهای ۵-۳-۲ تا ۵-۳-۴ توصیف شده است. در تمامی موارد، سازمان یا شکلی از فرایندهای مدیریتی را دارد یا اصلا هیچ فرایند مدیریتی وجود ندارد. بندهای زیر پیشنهادهایی برای پیاده‌سازی هر سه حالت و حالت بیان شده در بند ۵-۱ فراهم می‌کنند:

۵-۳-۲ هیچ استانداری به عنوان پایه‌ای برای سامانه مدیریت استفاده نشده است

آسان است تصور این‌که جایی‌که هیچ استانداردی پیاده‌سازی نشده است، رویه‌ها، فرایندها و خط‌مشی‌هایی وجود ندارد و در نتیجه وضعیتِ ساده‌ای است. هرچند، این امر تصوری غلط است.

تمامی سازمان‌ها شکلی از سامانه مدیریت را دارند. توصیه می‌شود به منظور دستیابی به انطباق با الزامات مشخص شده در یک یا هر دو استاندارد، این امر پذیرفته شود.

توصیه می‌شود تصمیم‌گیری با توجه به رتبه‌ای که دو سامانه مدیریت پیاده‌سازی خواهند شد، بر مبنای نیازهای کسب‌وکار و اولویت‌ها باشد. این که آیا رانهٔ اولیه در موقعیت رقابتی است یا نیاز به اثبات مقبولیت برای مشتری دارد می‌تواند در تصمیم‌گیری تاثیر داشته باشد.

تصمیم مهم دیگر این است که پیاده‌سازی هر دو استاندارد به‌صورت هم‌زمان یا به‌صورت پی‌درپی باشد. اگر پیاده‌سازی به‌صورت هم‌زمان باشد، یک استاندارد پیاده‌سازی می‌شود و سپس دامنه کاربرد گسترش می‌یابد تا شامل الزامات اضافی دیگر شود. به بند ۵-۳-۳ مراجعه شود. اگر فعالیت‌های پیاده‌سازی و تلاش‌ها بتوانند هماهنگ شوند و دوباره‌کاری کمینه شود، هر دو مورد ISMS و SMS می‌توانند به‌صورت هم‌زمان پیاده‌سازی شود. با این وجود، وابسته به طبیعت سازمان، می‌تواند آغاز نمودن با یک استاندارد و سپس گسترش دامنه کاربرد به دیگری به‌صورت محتاطانه انجام شود.

این ملاحظات در فرانامه‌های زیر نمایش داده شده‌اند:

الف- توصیه می‌شود سازمانی که خدماتی را فراهم می‌آورد با پیاده‌سازی استاندارد ISO/IEC 20000-1 آغاز کند و سپس از درس‌های فراگرفته در طول پیاده‌سازی آن، سامانه مدیریت را گسترش دهد به گونه‌ای

[1] - Scenarios

که شامل استاندارد ISO/IEC 27001 شود.

ب- توصیه می‌شود سازمانی که از تامین کنندگان (شامل طرفین دیگر) استفاده می‌کند، برای تحویل قسمت‌هایی از خدمات ابتدا بر استاندارد ISO/IEC 20000-1 تمرکز کند. استاندارد ISO/IEC 20000-1 بیشتر شامل الزاماتی برای مدیریت قسمت‌های دیگر شامل تامین کنندگان می‌شود. این امر امکان وضوح مدیریت تامین کنندگان و مسائل فرایند واپایشی را می‌دهد. سپس توصیه می‌شود سازمان به استاندارد ISO/IEC 27001 ارتقا یابد.

پ- توصیه می‌شود در سازمان‌های کوچک - وابسته به سطح اتکا بر مدیریت خدمت یا امنیت اطلاعات- بر یکی از دو استاندارد ISO/IEC 20000-1 و ISO/IEC27001 تمرکز داشته باشد.

ت- توصیه می‌شود سازمان‌های بزرگ که تحویل داخلی خدمات دارند، پیاده‌سازی را به‌صورت یک پروژه منفرد ساماندهی کنند. اگر این امر ممکن نبود، توصیه می‌شود به دو زیرپروژه موازی درون یک برنامه فراگیرِ[1] کار تقسیم شود. توصیه می‌شود هر زیر پروژه یک استاندارد را مدیریت کند و پیاده‌سازی‌ها را به‌صورت یک زیرپروژه مشترک یکپارچه سازد. اگر این خط‌مشی انتخاب شد، کسب اطمینان از اینکه پیاده‌سازی‌ها در صورت توسعه آن‌ها سازگار هستند، حیاتی است. این موضوع منجر به معرفی سربارهای افزوده و مقابله بیشتر با مخاطره می‌شود، بنابراین توصیه می‌شود که تنها اگر هیچ چاره‌ی دیگر وجود نداشت از آن استفاده شود.

ث- توصیه می‌شود هر سازمانی که سطح بالای اهمیت بر امنیت اطلاعات را به‌کار می‌گیرد، ابتدا ISMS ای را پیاده‌سازی کند که با الزامات مشخص شده در استاندارد ISO/IEC 27001 انطباق دارد. توصیه می‌شود گام بعدی گسترش سامانه مدیریت به منظور برآورده الزامات مشخص شده در استاندارد ISO/IEC 20000-1 با پشتیبانی از امنیت اطلاعات باشد.

گروه کاری یکپارچه‌سازی با برگزاریِ ملاقات‌های منظم در مدت پیاده‌سازی هردو سامانه مدیریت می‌تواند به حصول اطمینان از همسویی آن‌ها کمک کند.

۵-۳-۳ سامانه (مدیریت)ی هست که الزامات یکی از استانداردها را برآورده می‌کند

در موقعیتی که سامانه مدیریت تقریبا با الزامات مشخص شده در یکی از دو استانداردها انطباق دارد، توصیه می‌شود هدف اولیه یکپارچه نمودن الزامات استاندارد دیگر باشد. این موضوع باید بدون زحمت ناشی از حذف هیچ خدمت یا خطر امنیت اطلاعات خدمات انجام شود. هرچند، توصیه می‌شود سامانه مدیریت موجود به اجزای منحصر به فرد تقسیم شود. توصیه می‌شود این امر با مستندات موجود بازبینی شده توسط کارشناسان معرفی شده در این استاندارد و توسط هر کارشناسی که پیش از این در این استاندارد پیاده‌سازی شده، به‌صورت پیشرفته و به دقت طرح‌ریزی شود.

توصیه می‌شود این سازمان، خصیصه‌های سامانه مدیریت بنا شده را شناسایی کند، این شناسایی باید کمینه

[1] - Overarching

شامل موارد زیر باشد:

الف- دامنه کاربرد؛

ب- ساختار سازمانی؛

پ- خط‌مشی‌ها؛

ت- فعالیت‌های طرح‌ریزی؛

ث- مراجع و مسئولیت‌ها؛

ج- روش‌ها؛

چ- روشگان‌های[1] مدیریت مخاطره؛

ح- فرایندهای مرتبط؛

خ- روش‌های اجرایی؛

د- اصطلاحات و تعاریف؛

ذ- منابع.

توصیه می‌شود این خصیصه‌ها به منظور تعیین چگونگی به‌کاربستن آن‌ها در سامانهٔ یکپارچه مدیریت بازنگری شوند. اگر رویکرد دو-مرحله‌ای به گونه‌ای استفاده شود که در مرحله اول، سامانه مدیریت موجود در آن باشد و در مرحله‌ی دوم، پیاده‌سازی سامانه مدیریت دیگر باشد. توصیه می‌شود دامنه کاربرد برای مرحله‌ی دوم پیش از آغاز هر فعالیت پیاده‌سازیی دیگر تعریف و پذیرفته شود.

۵-۳-۴ سامانه‌های (مدیریت)ی جدا وجود دارند که الزامات هر یک از استانداردها را برآورده می‌کند

آخرین مورد ممکن است پیچیده‌ترین باشد. این مورد موضوع دامنه کاربرد را نشان می‌دهد؛ به بند ۵-۲ مراجعه شود. ممکن است سازمانی ISMS را در یکی از حوزه‌های سازمان و SMS را در حوزه دیگر پیاده‌سازی کند. این سازمان می‌تواند برای به‌کاربستن این یا آن استاندارد در دامنه کاربرد وسیع‌تر فعالیت‌ها تصمیم‌گیری نماید. در نقاطی از زمان، سامانه‌های مدیریت برای بعضی از فعالیت‌ها پیاده‌سازی می‌شوند. به‌صورت متناوب، دو سازمان می‌توانند برای ادغام شدن با یکدیگر طرح‌ریزی نمایند. یکی از آن‌ها انطباق با الزامات مشخص شده در استاندارد ISO/IEC 27001 را نشان می‌دهد در حالیکه دیگری انطباق با الزامات مشخص شده در استاندارد ISO/IE 20000-1 را نشان می‌دهد.

توصیه می‌شود از نقطه آغاز بازبینی شکل گیرد که به اکتساب موارد زیر کمک می‌کند:

[1] - Methodologies

الف- شناسایی و مستندسازی دامنه‌های کاربرد پیشنهادی و موجود که هر استانداردی به‌کار می‌برد، با توجه ویژه به تفاوت‌های آن‌ها؛

ب- مقایسهٔ سامانه‌های مدیریت موجود و در صورت وجود، تعیینِ جنبه‌هایی که به صورت متقابل ناسازگار هستند؛

پ- توسعهٔ مورد کسب‌وکاری برای روشن‌سازیِ منافع سامانه یکپارچه مدیریت؛

ت- آغاز به درگیر کردنِ ذینفعان هردو سامانه مدیریت با یکدیگر؛

ث- طرح‌ریزی بهترین رویکرد برای دستیابی به سامانهٔ یکپارچه مدیریت؛

۱- آغاز کردن با نگرش گسترده؛

۲- بازنگری این طرح در سطوح متنوع در سازمان برای افزودن جزئیات؛

۳- فراهم نمودن بازخورد و راه‌حل‌های پیشنهادی برای سطوح مناسب صلاحیت برای ایجاد امکان به منظور تصمیم‌گیری

با اینکه روش‌های زیادی از سامانه‌های یکپارچهٔ مدیریتی وجود دارد ضمن نگهداری انطباق، توصیه می‌شود مرحله‌ی طرح‌ریزی گسترده کامل شده باشد.

۶ ملاحظات یکپارچهٔ پیاده‌سازی

۶-۱ کلیات

در تمامی موارد، توصیه می‌شود هدف سازمان تولید نمودن سامانه یکپارچه مدیریت با قابلیت رشد باشد که قادر به انطباق با الزامات مشخص شده در هردو استاندارد است. هدف، مقایسه استانداردها یا تعیین نمودن درست و بهترین نیست. جایی که بین دیدگاه‌ها ناسازگاری وجود دارد، توصیه می‌شود به روشی حل شود که الزامات مشخص شده در هر دو استاندارد را برآورده کند و اطمینان حاصل شود که سازمان به بهبود مستمر در ISMS و SMS می‌رسد. توصیه می‌شود سامانهٔ یکپارچه مدیریت مطلوب بر مبنای کاراترین رویکرد از هر دو استاندارد به‌کاربسته شده به‌صورت مناسب باشد. این امر همچنین با استفاده از جزئیات افزوده در یک استاندارد برای تکمیل دیگری پشتیبانی شده است. توصیه می‌شود دقت زیادی شود که هر چیز لازم برای انطباق با هر دو استاندارد، حفظ شود.

توصیه می‌شود قابلیت ردیابی مستند بین سامانهٔ یکپارچه مدیریت و الزامات هر استاندارد دیگر نگهداشته شود. به منظور کاهش تلاش، مجموعه‌ای مجزا از مستندات می‌تواند برای سامانهٔ یکپارچه مدیریت ایجاد شده باشد. برای پشتیبانی از این، سازمان قادر به ایجاد مستندسازی قابلیت ردیابی مانند ماتریس قابلیت ردیابی است. این صراحت نشان‌دهنده‌ی چگونگی انطباق سامانهٔ یکپارچه مدیریت با الزامات هر استاندارد است. مزایای این رویکرد این است که قادر به نمایش ساده‌تر انطباق در ممیزی‌ها و بازبینی‌ها است. ازجمله‌ی این

مزایا این است که قادر به ردیابی کردن فعالیت‌هایی است که برای نمایش انطباق با هر استانداری ضروری هستند.

۶-۲ چالش‌های بالقوه

۶-۲-۱ کاربرد و معنای دارایی

در این بند، تفاوت‌ها و شباهت‌های استفاده و معنای دارایی در استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 بحث می‌شوند. دربارهٔ چگونگی تطبیق دادنِ دو استاندارد، پیشنهاداتی ارائه می‌شود.

دارایی در استاندارد ISO/IEC 20000-1، متفاوت با دارایی استاندارد ISO/IEC 27001 است. دارایی، اصطلاحی تعریف شده در استاندارد ISO/IEC 20000-1 یا استاندارد ISO/IEC 27001 نیست، لذا در معنای رایج زبان انگلیسی مقادیر بعضی چیزها استفاده شده است. در بعضی از بندهای استانداردISO/IEC20000-1 استفاده از دارایی به دارایی‌های اقتصادی پیوند یافته است مانند مجوزهای نرم‌افزاری. در بندهای دیگر، دارایی‌ها به‌صورت دارایی‌های اطلاعاتی نسبت داده می‌شوند. در مقابل، استاندارد ISO/IEC 27001 برمبنای مفهوم حفاظت اطلاعات است. کلمه‌ی دارایی در استاندارد ISO/IE 20000-1 در معنای رایج انگلیسی خود استفاده می‌شود: هرچیزی که باارزش و مفید در نظر گرفته می‌شود، مانند مهارت، کیفیت یا شخص و غیره. هم چنین استاندارد ISO/IEC 20000-1 از اصطلاح تعریف شده، قلمِ پیکربندی (CI)[1]، به‌صورت عنصر استفاده می‌کند که به منظور تحویل خدمات نیاز به واپایش شدن دارد. لذا توصیه می‌شود سازمان، CI ای را تعریف کند که برای اهداف خود است و نیازهای آن را برای کارایی در نظر بگیرد. اطلاعات می‌تواند در این تعریف شامل شود. در استاندارد ISO/IEC 20000-1، دادگان پیکربندی مدیریت (CMDB) [2] انباره داده‌ای از تمامی CI ها و روابط داخلی آن‌ها است. دارایی‌های بعضی از سازمان‌ها، در CMDB نخواهد بود (به طور مثال، PC ها به منظور تحویل یا دسترسی به خدمات استفاده نشده‌اند). به طور برابر، بعضی از CI ها ممکن است با استاندارد ISO/IEC 20000-1 دارایی در نظر گرفته نشوند، به طور مثال، مردم. دارایی‌ها در استاندارد ISO/IEC 20000-1 به‌صورت عادی دارای ارزش مالی هستند.

در استاندارد ISO/IEC 27001، تمرکز بر ارزیابی مخاطره‌ی امنیت اطلاعات و برطرف‌سازی مخاطره‌ای است که برای تمامی اطلاعات درون دامنه کاربرد ISMS به‌کار رفته است. شکل اطلاعات نامرتبط است و می‌تواند به‌صورت دست‌نویس، الکترونیکی و... باشد. در نتیجه، اطلاعات یا منابع استفاده شده برای ساماندهی اطلاعات می‌تواند CIها باشد. به طور مثال، هادی داده می‌تواند CI باشد. با اینکه هادی، اطلاعات نیست، هادی منبع استفاده شده برای حمل اطلاعات و لذا مربوط به ارزیابی مخاطره در استاندارد ISO/IEC 27001 است. برای سامانه یکپارچه مدیریت، اطلاعات می‌تواند توسط خدمات استاندارد ISO/IEC 20000-1 استفاده شود.

---

[1] - Configuration Item

[2] - Configuration Management DataBase

در هیچ یک از استانداردها نیاز نیست که هر CI یا نمونه‌ی اطلاعات به‌صورت جداگانه فهرست شود. می‌توانند به انواعی گروه‌بندی شوند مانند سخت‌افزار یا مستندات. به عنوان قسمتی از این فعالیت، توصیه می‌شود توصیف آن‌ها تا جای ممکن سازگار باشد، تا انطباق با هر دو استاندارد را ساده و آسان کند. به طور مثال، در آغاز هر کار یکپارچه، توصیه می‌شود دربارهٔ روش رده‌بندی و شناسایی تصمیم‌گیری شود. این کار به منظور کسب اطمینان از این است که منابع غیرمبهم می‌توانند دارایی‌ها را ایجاد کنند. اگر اصطلاح دارایی برای اشاره به اطلاعات به‌کار رود، توصیه می‌شود دارایی‌های مشخص با برچسبی افزوده داده شوند تا از حالت آن‌ها برای شناسایی به‌صورت CI ها یا دارایی‌هایی اقتصادی در استاندارد ISO/IEC20000-1 اطمینان کسب شود (به پیوست ب مراجعه شود).

۶-۲-۲ طراحی و انتقال خدمات

استاندارد ISO/IEC 20000-1:2011 در بند ۵ برای طراحی و انتقال خدمات جدید یا تغییریافته، الزاماتی را در خود جای داده است. هیچ بند معادلی به‌صورت مستقیم در استاندارد ISO/IEC 27001 وجود ندارد، با این حال، نیاز است تغییرات در مسائل داخلی و خارجی در مدت بازنگری مدیریت ISMS (استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، بند ۹-۳) در نظر گرفته شود و مفاهیم دیگر طراحی، انتقال و تحویل خدمت در پیوست الف استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، جای گرفته‌اند. هر چند، توصیه می‌شود سامانه یکپارچه مدیریت از امنیت اطلاعاتی که در مدت مراحل طرح‌ریزی طراحی و انتقال خدمات جدید یا تغییریافته در نظر گرفته‌اند، اطمینان کسب کنند. موضوعاتی که توصیه می‌شود در نظر گرفته شوند شامل ارزیابی تاثیر خدمات جدید یا تغییر کرده در هر دوی واپایش‌های ایمنی خدمات و اطلاعات موجود است (به بند 6.6.2 استاندارد ISO/IEC 20000-1:2011 مراجعه شود). توصیه می‌شود اینکار برای خاتمه‌ی خدمات انجام شود.

توصیه می‌شود طرح‌ریزی تمامی خدمات جدید یا تغییریافته شامل پیامدهای امنیت اطلاعات باشد. توصیه می‌شود اینکار صرف نظر از اینکه آیا خدمت درون دامنه کاربرد ISMS قرار می‌گیرد یا نه انجام شود.

۶-۲-۳ ارزیابی و مدیریت مخاطره

بند ۶-۱ و بند ۸ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، الزامات ارزیابی و برطرف‌سازی جنبه‌های مخاطره‌های متناظر با امنیت اطلاعات را مشخص می‌کند. این الزامات محدود به مخاطرات متناظر با ISMS نیستند و شامل ارزیابی و برطرف‌سازی مخاطرات و دیگر جنبه‌های مدیریت مخاطرات امنیت اطلاعات می‌باشند. بند ۶-۱ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، جزئیاتی پیرامون چگونگی استخراج، ارزیابی و برطرف‌سازی مخاطرات امنیت اطلاعات فراهم می‌کند.

با اینکه مخاطرات در استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 در نظر گرفته شده‌اند، طبیعت این مخاطرات متفاوت است. استاندارد ISO/IEC 20000-1 مخاطراتی را برای SMS و خدمات در نظر می‌گیرد در حالیکه استاندارد ISO/IEC 27001 مخاطرات امنیت اطلاعات و تاثیر آن بر سازمان را در نظر

می‌گیرد. معیار برای ارزیابی و برطرف‌سازی مخاطرات متفاوت است و وابسته به این است که برای ارائه‌ی خدمت یا امنیت اطلاعات، مخاطرات آن مشخص است یا خیر. هرچند، روش استفاده شده برای شناسایی مخاطرات می‌تواند در هر دو مورد یکسان باشد. بعضی از مخاطرات در نظر گرفته شده توسط استاندارد ISO/IEC 20000-1، به طور مثال، مخاطره کارپرداز بدون توجه به هزینه‌های متناظر با قرارداد سطح خدمت (SLA)، از دیدگاه استاندارد ISO/IEC 27001 مخاطره در نظر گرفته نشده است. لذا، مخاطرات شناسایی شده با استفاده از استاندارد ISO/IEC 20000-1 نمی‌تواند مربوط به امنیت اطلاعات باشد و برعکس.

همچنین مالکیت مخاطره نیز می‌تواند بین دو رویکرد متفاوت باشد. به طور مثال، در استاندارد ISO/IEC 20000-1، سازمان فراهم‌ساز خدمت به ندرت تمامی مخاطرات را می‌پذیرد. مشتری می‌تواند این انتظار را داشته باشد که مخاطرات باقی‌مانده را به عنوان قسمتی از SLA آن‌ها یا طرح تداوم خدمات بپذیرد. در استاندارد ISO/IEC 27001، اهمیت مالکیت مخاطره به‌صورت واضح مورد بررسی قرار نگرفته است اما در عمل، سازمان مسئول تمامی مخاطرات امنیت اطلاعات است.

به دلیل تفاوت‌های الزامات برای مدیریت مخاطره بین دو استاندارد، سوء تفاهم‌هایی در گزینه‌های مواجهه مخاطرات پدید می‌آید. در زمان طرح‌ریزی کردن پیاده‌سازی یکپارچهٔ هر دو استاندارد، توصیه می‌شود سازمان‌ها به تفاوت‌های مخاطرات و تاثیر این تفاوت‌ها بر بررسی مخاطرات به خوبی بیندیشند.

توصیه می‌شود سازمان یکی از رویکردهای توصیف شده در زیر را اتخاذ کند.

الف- از روشی متداول برای مدیریت مخاطره، شامل ارزیابی مخاطره، برای هر دو استاندارد استفاده شود و از کپی‌برداری اجتناب شود. برای مثال، مخاطره‌ی کاهش در دسترس بودن دارایی اطلاعاتی ممکن است توسط قسمت‌های متفاوت سامانه یکپارچه مدیریت به اشتراک گذارده شده باشد. موثرترین رویکرد، اجتناب از کپی‌برداری است.

ب- از روشگان جداگانه ارزیابی مخاطره برای دو استاندارد استفاده شود. اگر این گزینه انتخاب شد، توصیه می‌شود سازمان از اصطلاحاتی استفاده کند که بین ارزیابی مخاطره‌ی SMS و خدمات ISMS و ارزیابی مخاطرات امنیت اطلاعات تفاوت قائل شود.

پ- از رویکرد متداولی برای ارزیابی و برطرف‌سازی کردن مخاطراتی استفاده شود که هم بر امنیت اطلاعات و هم بر مدیریت خدمت تاثیر دارد و روشگان ارزیابی جداگانه‌ی مخاطره برای مخاطراتی که برای امنیت اطلاعات و مدیریت خدمت مشخص هستند.

هر رویکردی که به‌کار گرفته شود، تقسیم‌کننده‌ی ارزیابی و برطرف‌سازی مخاطره برای در نظر گرفتن جداگانه‌ی مخاطراتی است که هم بر امنیت اطلاعات و هم بر مدیریت خدمت تاثیر می‌گذارند و مخاطراتی که بر امنیت اطلاعات یا مدیریت خدمت تاثیر می‌گذارند می‌توانند سامانه مدیریت را به‌صورت کارا بهبود ببخشند.

در موقعیتی که ارزیابی و برطرف‌سازی مخاطره برای سازمان حیاتی است، توصیه می‌شود اولویت با

پیاده‌سازی استاندارد ISO/IEC 27001 باشد تا از مزیت‌های الزامات ارزیابی و برطرف‌سازی مخاطره استفاده شود. چنانچه هر گزینه‌ای استفاده شود، توصیه می‌شود سازمان از اصطلاحات سازگار و واضح استفاده کند. این امر ممکن است نیاز به بیان نمودن الزامات یک یا هر دو استاندارد به‌صورت متفاوت با نسخه‌های مورد انتظار داشته باشد. هرچند، توصیه می‌شود سازمان هنوز هم از قابلیت اطمینان الزامات مشخص در هر دو استاندارد اطمینان کسب کند.

۶-۲-۴ تفاوت‌ها در سطوح پذیرش مخاطرات

در موقعیتی که مشتری داده‌ها یا سامانه‌های خود را به طرف سومی سپرده است، می‌تواند تفاوت‌هایی بین سطح پذیرش مخاطره‌ی مشتری و آن طرف سوم وجود داشته باشد. در این استانداردها این موضوع به روشنی پوشش داده نشده است، اما توصیه می‌شود که سازمان از مسائل آگاهی داشته باشد و با توجه به سطوح مخاطراتی که توسط طرف‌های متفاوت واپایش شده است، تصمیم روشنی اتخاذ کند.

مسائل کلیدی در زیر توصیف شده‌اند.

الف- مشتری دارای دیدگاهی با توجه به سطح امنیتی خواهد بود که برای اطلاعاتش که تحت واپایش طرف سوم است، قابل‌پذیرش است. این امر ممکن است با سطح امنیتی که طرف سوم آن را کافی در نظر می‌گیرد، مطابقتی نداشته باشد.

ب- طرف سوم[1] همیشه دارای اطلاعات خودش خواهد بود، به طور مثال، ثبت‌های مالی. طرف سوم دیدگاهی با توجه به سطح امنیت پذیرش برای این اطلاعات خواهد داشت.

پ- ممکن است مشتری و طرف سوم در محیط‌های اجرایِ قانونی و تنظیمیِ متفاوت درگیر باشند که با توجه به کشور یا بخش بازار، متغیر است. این امر می‌تواند منجر به دیدگاه‌های متفاوت امنیت اطلاعات یا مخاطرات شود.

توصیه می‌شود انتظارات و مسئولیت‌های امنیت اطلاعات مشتری‌ی سازمان و طرف‌های سوم در اولین فرصت‌های ممکن مورد بحث قرار گیرد. این بحث‌ها برای هر دو در مدت پذیرش دامنه کاربرد پیاده‌سازی پروژه و در هنگام بنیاد نهادن واپایش‌های عملیات برای خدمات موجود دارای اهمیت است. توصیه می‌شود قبل از پیاده‌سازی به‌صورت مطلوب هر تعارضی شناسایی شود و تصمیم‌گیری انجام شود و مورد پذیرش قرار گیرد.

۶-۲-۵ مدیریت رخداد و مسئله[2]

اولین نقطه مقایسه، اصطلاحات تخصصی آن است. در استاندارد ISO/IEC27001، اصطلاح رویدادهای ناخواسته مورد توجه، رخداد امنیت اطلاعات است. در مقابل، در استاندارد ISO/IEC 20000-1 چندین اصطلاح مشخص با مدیریت رخداد پیوند دارد. برای مثال، رخداد، رخداد امنیت اطلاعات، مسائل، خطای

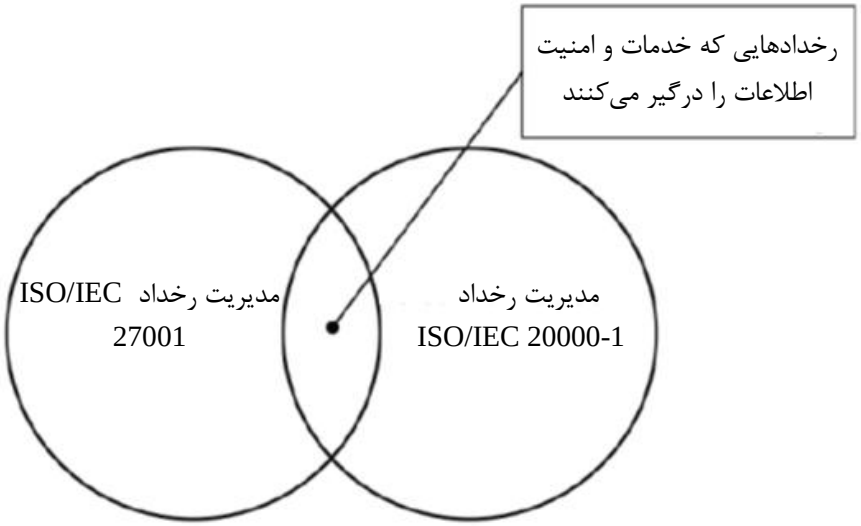
[1] - Third party
[2] - Incident and problem management

شناخته شده و رخداد مهم (به پیوست ب مراجعه شود). این‌ها می‌توانند تمامی رخدادهای امنیتی اطلاعات مطابق با استاندارد ISO/IEC 27001 باشند که وابسته به مشخصات آن است.

استاندارد ISO/IEC 27001 فرایندی منفرد برای مواجهه با تمامی رخدادهای امنیت اطلاعاتی مشخص می‌کند.

استاندارد ISO/IEC 20000-1 دارای سازوکارهای مختلفی برای مدیریت این رخدادها است؛ مانند مدیریت درخواست رخداد و خدمات، روش‌اجرایی عمده رخداد و مدیریت مساله. در استاندارد ISO/IEC 20000-1، رویداد می‌تواند توسط بیش از یکی از این فرایندها و روش‌های اجرایی در مدت چرخه عمر مدیریت شده باشد. استاندارد ISO/IEC 20000-1 از تعاریف ISO 9000 برای روش‌اجرایی به‌صورت «روشی مشخص برای انجام اقدامات یا فرایند» استفاده می‌کند. برای استاندارد ISO/IEC 20000-1 فرایند در سطح بالاتری از روش‌اجرایی است، با روش‌های اجرایی پشتیبانی کننده از فرایند.

شکل ۲ رابطه‌ی بین مدیریت امنیت اطلاعات در استاندارد ISO/IEC 27001 و مدیریت رخداد در استاندارد ISO/IEC 20000-1 نشان داده شده است.



شکل ۲- نمایش رابطه بین استانداردها برای مدیریت رخداد

رویدادهایی وجود دارند که استاندارد ISO/IEC 27001 به‌صورت رخداد امنیت اطلاعات آن‌ها را طبقه‌بندی می‌کند، اما استاندارد ISO/IEC 20000-1 آن‌ها را به‌صورت رخداد در نظر نمی‌گیرد. در ادامه دو مثال ارائه شده است.

الف- سندی محرمانه دربارهٔ بازاریابی محصول بعد از ساعت کاری روی میز یافت می‌شود که مغایر با خط‌مشی امنیت اطلاعات است. این سند به خدمات یا تحویل خدمات ارتباطی ندارد.

ب- قفل در دفتر مشتری شکسته شده باشد. این رویداد می‌تواند در IDO/IEC 27001 به عنوان رویداد در نظر گرفته شود. هرچند، در دامنه استاندارد ISO/IEC 20000-1 قرار نمی‌گیرد، مگر اینکه اطلاعات مربوط به الزامات در استاندارد ISO/IEC 20000-1:2011 در ۶-۶ با خدمات پشتیبانی شده توسط SMS روی رویداد تاثیر داشته باشد.

همچنین، رویدادهایی وجود دارند که استاندارد ISO/IEC 20000-1 به‌صورت رخداد آن‌ها را طبقه‌بندی می‌کند؛ اما خارج از دامنه کاربرد استاندارد ISO/IEC 27001 هستند. در زیر مثال‌هایی ارائه شده است:

الف- نگهداشت زمانبدی‌شده خارج از حدود SLA

ب- کاربر رخدادی را به دلیل عملکرد آهسته خدمات گزارش می‌دهد.

اشتراک ابتدایی بین تعاریف «رخداد» به چیزی مربوط می‌شود که استاندارد ISO/IEC 20000-1 از آن به «رخدادهای امنیت اطلاعات» اشاره می‌کند که می‌تواند به دلیل از دست رفتنِ محرمانگی، یکپارچگی و دسترسی‌پذیری مرتبط به خدمات باشد.

به منظور تطبیق دادن این دیدگاه‌ها، توصیه می‌شود سازمان دربارهٔ چگونگی ساماندهی کردن مدیریت این رخدادها که در دامنه کاربرد هردو سامانه مدیریت هستند، تصمیم‌گیری نماید.

مدیریت مساله در استاندارد ISO/IEC 20000-1 به‌صورت فرایندی برای شناسایی ریشه‌ی علت یک یا تعداد بیشتری رخداد برای کمینه کردن یا اجتناب از تاثیر رخدادها است. در استاندارد ISO/IEC 20000-1، این فرایندی مشخص و جداگانه است. در استاندارد ISO/IEC 27001، مدیریت مساله به‌صورت آشکار پوشش داده نشده است، با این حال، این موضوع در الزامات مدیریت رخداد امنیت اطلاعات و حذف مخاطره اشاره شده است.

در سامانه‌ای با مدیریت یکپارچه، توصیه می‌شود فرایند مدیریت مساله تعریف شده باشد. اگر ISMS قبل از SMS پیاده‌سازی شده باشد، می‌تواند برای یکپارچه نمودن بهترین عمل‌های SMS برای مدیریت مساله به‌صورت قسمتی از ISMS مفید باشد، به دلیل مزایای آن برای سامانه‌های مدیریت.

هر دوی استانداردها برای تحلیل نمودن داده و سیر پیاده‌سازی رخداد نیاز به سازمان دارند.

توصیه می‌شود رخدادهایی که مخاطره‌ی امنیت اطلاعات را درگیر می‌کنند، به‌صورت رخدادهای امنیت اطلاعات طبقه‌بندی شوند. این موضوع به‌صورت یکسان برای قابلیت اطمینان هر دو استانداردهایی مهم است که توصیه می‌شود فرایند مدیریت رخداد نیازها را برای مقابله با الزامات اضافی برای مدیریت امنیت اطلاعات در استاندارد ISO/IEC 27001 انعکاس ببخشد.

لازم به ذکر است که واپایش در بند الف-۱۶-۶-۱-۶ از استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، یادگیری از رخدادهای امنیتی و لذا اشتراک جزئی با مدیریت مساله را در استاندارد ISO/IEC 20000-1:2001,8-2 پوشش می‌دهد. علاوه بر این، توصیه می‌شود شناسایی و ارزیابی آسیب‌پذیری‌های مورد نیاز برای ارزیابی مخاطره‌ی امنیت اطلاعات استاندارد ISO/IEC 27001 به‌صورت روند تحلیل داده‌ای در نظر

گرفته شود که می‌تواند به‌صورت ورودی برای مدیریت مساله استفاده شود.

نقطه دوم مقایسه، اهمیت پاسخ به رخداد است. توصیه می‌شود بعد از اینکه رخداد امنیت اطلاعات بر خدمات تاثیر گذاشت، هر سازمانی دارای عملیات خدماتی ترمیم سریع باشد. هرچند، این امر سبب کاهش بررسی احتمالاتی می‌شود که به منظور درک علت رخداد امنیتی انجام می‌شود. توصیه می‌شود در زمان یکپارچه نمودن SMS و ISMS دقت کافی به‌کار رود تا از الزامات رخدادهای مدیریت امنیت اطلاعات اطمینان کافی کسب شود. به طور مثال، واپایش‌های امنیت اطلاعات می‌تواند شامل جمع‌آوری، نگهداری و تدارک دیدن مدرک برای اهداف قانونی شود. علاوه بر این، هردوی استانداردها با الزامات کاربردپذیر قانونی و منظم، مطابقت دارند.

دربارهٔ رخدادهای امنیتی، الزامات برای جمع‌آوری مدرک می‌تواند به این معنا باشد که خدمات تحت تاثیر قرار گرفته نمی‌توانند درون هدف‌های قابل خدمات بازسازی شوند. استاندارد ISO/IEC 20000-1 الزاماتی برای فراهم کنندگان خدمات مشخص می‌کند تا فوریت و تاثیر رخداد را در نظر بگیرند. این موضوع می‌تواند به این معنا باشد که پیش از اینکه رخداد امنیت اطلاعات حل شود زمان بیشتری برای جمع‌آوری مدرک مورد نیاز است. توصیه می‌شود اولویت‌های تخصیص داده شده برای حل نمودن موضوع؛ اهمیت مدرک جمع‌آوری امنیت اطلاعات را که می‌تواند از طرف دیگر توسط بازسازی خدمات از بین رود را در نظر بگیرد.

در بعضی از موارد، برمبنای تعریف رخداد عمده مطابق با مشتری مشخص در استاندارد ISO/IEC 20000-1:2011,8، رخداد امنیت اطلاعات می‌تواند رخداد عمده باشد. مطابق با الزامات گزارش خدمات در استاندارد ISO/IEC 20000-1:2011,6-2 و الزامات مدیریت رخدادهای عمده در استاندارد ISO/IEC 20000-1:2011,8-1، مدیریت مناسب از تمامی رخدادهای عمده، آگاهی دارد. این امر شامل رخدادهایی می‌شود که رخدادهای امنیت اطلاعات محسوب می‌شوند. این امر، افرادی که به‌صورت مناسب آموزش دیده اند و مسئول‌اند را برای مدیریت رخداد امنیت اطلاعات منصوب می‌کند. توصیه می‌شود بعضی از رخدادهای امنیت اطلاعات با استفاده از استاندارد فرایند رخداد بزرگ، ساماندهی نشود و توسط کارکرد مدیریت امنیت اطلاعات ساماندهی شوند، به طور مثال، تجاوز داخلی امنیتی که نیاز به بررسی پلیس و بازرسی قانونی دارد. این نوع از رخدادها باید به گروه‌های کوچک‌تری از حد متداول محدود شوند.

توصیه می‌شود رخداد عمده به‌صورت عادی اعلان نشود تا برای جمع‌آوری مدرک دربارهٔ رخداد امنیت اطلاعاتی امکان تاخیر در حل کردن ایجاد شود. برای مثال، اگر وب‌گاه ساماندهی پرداخت‌های مشتری در خطر نقض باشد. توصیه می‌شود جمع‌آوری مدرک و زمان‌های ترمیم خدمات به‌صورت کافی در الزامات خدمت، فهرست خدمات و در قراردادهای سطح خدمات (SLA) پوشش داده شود.

تعریف استاندارد ISO/IEC 20000-1 از امنیت اطلاعات از کلمه‌ی «دسترسی‌پذیری[1]» و تعریف استاندارد ISO/IEC 27001 از کلمه‌ی «در دسترس بودن[2]» استفاده می‌کند. این تفاوت به این دلیل است که کلمه‌ی

1- Accessibility
2- Availability

«در دسترس بودن» در دو استاندارد به‌صورت متفاوت تعریف شده است، همان‌طور که در پیوست ب توصیف شده است.

۶-۲-۶ مدیریت تغییر

بند ۷-۵-۳ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، نیاز به تغییراتی برای مستند کردن اطلاعات مورد واپایش مربوط به ISMS دارد. بند ۸-۱ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، نیاز به سازمانی برای واپایش تغییرات طرح‌ریزی شده دارد.

بندهای الف-۱۵-۲-۲، ۱۴-۲-۴، ۱۴-۲-۳، الف-۱۴-۲-۲، الف-۱۲-۱-۲ از استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، مدیریت تغییرات را توصیف می‌کند. این بندها به سازمان امکان توسعهٔ روش‌های پیاده‌سازیی برای نیل به نیازهای مشخص را می‌دهند.

بند ۹-۲ در استاندارد ISO/IEC 20000-:2011 شامل الزامات مربوط به مخاطره است. این الزامات توسط بندهای ۶-۶-۳ و ۶-۶-۲ شامل الزاماتی برای ارزیابی اثر تغییرات مورد تقاضا است تا اثر آن‌ها را بر واپایش‌های امنیت اطلاعات موجود در نظر بگیرد.

به منظور اطمینان از اینکه الزامات مدیریت تغییر برآورده شده‌اند، توصیه می‌شود فهرستی برای ارزیابی اثر یا مرور پس از پیاده‌سازی به‌صورت قسمتی از سامانهٔ مدیریت یکپارچه بر مبنای الزامات مشخص شده در استاندارد ISO/IEC 20000-1 ایجاد شود. توصیه می‌شود که از اینکه تمامی انواع مخاطرات امنیت اطلاعات به‌صورت قسمتی از فرایند مدیریت تغییرات مرور شده‌اند، اطمینان کسب شود.

۶-۳ بهره بالقوه[1]

۶-۳-۱ استفاده از چرخه‌ی طرح-انجام-بازبینی-اقدام[2]

استاندارد ISO/IEC 20000-1 به‌صورت واضح به چرخه‌ی طرح-انجام-بازبینی-اقدام (PDCA) اشاره می‌کند. با وجود اینکه استاندارد ISO/IEC 27001 این چرخه را به روشنی بیان نمی‌کند، بندهای اصلی آن پیرامون چرخه‌ی PDCA ساخته شده‌اند. این موضوع می‌تواند به سازمان کمک کند، به گونه‌ای که می‌تواند از جزئیات استاندارد ISO/IEC 20000-1 به منظور پشتیبانی کردن از پیاده‌سازی سامانهٔ مدیریت یکپارچه استفاده نماید. عنصرهای چرخه‌ی PDCA می‌تواند برای ساختار استاندارد ISO/IEC 27001 به‌صورت مناسب نگاشته شود.

۶-۳-۲ مدیریت و گزارش سطح خدمات

گزارش خدمات مبنای وسیع‌تری از اقدامات نسبت به اقدامات مشخص شده برای مدیریت سطح خدمات را پوشش می‌دهد. با این حال، گزارش خدمات می‌تواند مدیریت امنیت اطلاعات را توسط هدف‌های خدماتی

1- Potential gain

2 - Plan-Do-Check-Act cycle

برای رخدادهای امنیت اطلاعاتی پشتیبانی کند که در گزارش خدمات، سنجیده و استفاده شده‌اند.

استاندارد ISO/IEC 20000-1:2011 در بند ۶-۲ و بولت b توصیه می‌کند که گزارش خدمات شامل اطلاعات مربوط دربارهٔ رویدادهای مهم باشد، مانند رخدادهای مهم و غیر مشابه. خروجی‌ها از فرایند گزارش خدمات استاندارد ISO/IEC 20000-1 می‌تواند امتیازی بزرگ برای نگهداشت و بهبود امنیت اطلاعات باشد.

هنگام پیاده‌سازی استاندارد ISO/IEC 27001، جزئیات واپایش‌های امنیت اطلاعات تعریف شده‌اند و توصیه می‌شود اثربخشی این واپایش‌ها سنجیده شود (استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، بند ۹-۱). این موضوع همچنین شانسی را برای یکپارچه شدن با فرایند گزارش خدمات استاندارد ISO/IEC 20000-1:2011 بند ۶-۲ فراهم می‌کند به گونه‌ای که اطلاعات مربوط و زمانی بتوانند برای نگهداشت و بهبود امنیت اطلاعات استفاده شوند. اگر سطوح مقبولیت واپایش امنیت اطلاعات مرتبط و آماره‌های رخداد درون این گزارش‌ها ثبت شده باشند، مشتریان می‌توانند دارای درک بهتری از پیاده‌سازی درست خدمات و SMS؛ شامل فرایندهای مدیریت خدمت باشد.

توصیه می‌شود گزارش‌ها برای پشتیبانی از ISMS و SMS چه برای استفاده داخلی یا برای مشتریان، با در نظر گرفتن ملاحظات طراحی شوند.

۶-۳-۳ تعهدات مدیریت

استاندارد ISO/IEC 27001 امنیت اطلاعات را در رابطه با «طرف‌های ذی‌نفع» توصیف می‌کند. این‌ها طرف‌هایی با علایق گسترده‌ای در سازمانی هستند که در آن ISMS پیاده‌سازی شده است. این طرف‌ها می‌توانند شامل، کارمندان، سهامداران، مشتریان و مراجع صلاحیت‌دار تنظیمی[1] یا کل ملت باشند. استاندارد ISO/IEC 20000-1 به مشتریان و طرف‌های ذی‌نفع اشاره می‌کند. طرف‌های دی نفع شخص یا گروهی هستند که دارای علایقی مشخص در پیاده‌سازی یا موفقیت اقدامات فراهم‌کننده خدمت می‌باشند. «طرف‌های ذی‌نفع» در استاندارد ISO/IEC 20000-1 مشابه «طرف‌های ذی‌نفع» در استاندارد ISO/IEC 27001 هستند.

تعهدات مدیریتی برای ایجاد کردن SMS موثر مورد نیاز است. این امر شامل کسب اطمینان از این است که رابطه‌ی با مشتریان و دیگر طرف‌های ذی‌نفع موفقیت‌آمیز است. تعهدات مدیریتی مشخص شده در استاندارد ISO/IEC 27001 می‌تواند رویکرد متمرکز بر مشتری در استاندارد ISO/IEC 20000-1 را پشتیبانی کند.

استاندارد ISO/IEC 20000-1 مشخص می‌کند که هنگام نمایش بهبودهای مدیریتی، توصیه می‌شود سازمان مسئولیت برای بهبودهای مدیریت برای SMS و خدمات را به‌کار گیرد تا نقشی مشخص را پیاده‌سازی نماید. در مقابل، استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، در بند ۵-۱ برای پیشرفت مستمر به مدیریت ارشد نیاز دارد، در حالیکه بند ۵-۲ نیاز به مدیریت ارشد برای به‌کاربردن آن برای پیشرفت مستمر است. استاندارد ISO/IEC 27001:2013 در بند ۶-۱-۱ و ۷-۱ به جنبه‌های مختلف پیشرفت مستمر مدیریت

1 - Regulatory authorities

سازمان اشاره می‌کند در بند ۱۰-۲ اشاره می‌کند که سازمان باید پیشرفت مستمری را برای ISMS خود داشته باشد.

توصیه می‌شود الزامات استاندارد ISO/IEC 20000-1برای تخصیص روشن مسئولیت برای مدیریت کردن پیشرفت‌ها استفاده شود تا از مدیریت پیشرفت‌ها که برای امنیت اطلاعات به نقشی مشخص تخصیص داده شده است؛ اطمینان کسب شود.

۶-۳-۴ مدیریت ظرفیت

در بند ۶-۵ در استاندارد ISO/IEC 20000-1:2011 مدیریت ظرفیت شامل محدوده‌ی وسیع‌تری از مفاهیم ظرفیتی نسبت به استاندارد ISO/IEC 27001 است، بنابراین بعضی از الزامات مشخص شده در استاندارد ISO/IEC 20000-1 می‌تواند برای پشتیبانی از پیاده‌سازی استاندارد ISO/IEC 27001 استفاده شود. به طور مثال، مدیریت ظرفیت به همان صورت مشخص شده در استاندارد ISO/IEC 20000-1 به ظرفیت فنی و ظرفیت منبع انسانی اعمال می‌شود.

در استاندارد ISO/IEC 27000:2014 بند ۲-۱۰ در دسترس بودن برای معنا کردن در دسترس بودن و قابل استفاده بودن تعریف شده است. مدیریت ظرفیت در استاندارد ISO/IEC 20000-1:2011 بند ۶-۵ هر دوی این مفاهیم در دسترس بودن را پشتیبانی می‌کند. به طور مثال، اگر ظرفیت ناکافی وجود داشته باشد، عضو خدماتی می‌تواند غیرقابل دسترس باشد، به طور مثال اگر ذخیره کردن پوشه‌ای ممکن نباشد چون ظرفیت ذخیره‌سازی خیلی کمی موجود است. عضو خدماتی می‌تواند آن‌قدر کند باشد که غیرقابل استفاده باشد به طور مثال، زمان پاسخ به دلیل خیلی کم بودن ظرفیت شبکه.

توصیه می‌شود سازمان از این تفاوت‌ها در زمان ارجاع دادن به الزامات بین دو استاندارد آگاه باشد. توصیه می‌شود سازمان نیاز برای ارجاع متقاطع بین بند ۴-۳ و ۶-۵ در استاندارد ISO/IEC 20000-1;2011 و بندهای مربوط در استاندارد ISO/IEC 27001 را در نظر بگیرد. به پیوست الف مراجعه شود. به طور مثال، توصیه می‌شود الزاماتی که شامل تاثیر قانون، نظم دهندگی، تغییرات قراردادی یا سازمانی در طرح ظرفیت هستند و در ۶-۵ در استاندارد ISO/IEC 20000-1 مشخص شده‌اند با A-12-1-3 در استاندارد ISO/IEC 27001 ارجاع متقابل داده می‌شوند.

۶-۳-۵ مدیریت مخاطره‌ی طرف سوم

در استاندارد ISO/IEC 27001، طرف سوم، مانند مشتری یا تامین کننده، درون دامنه کاربرد ISMS است و منبع بالقوه‌ی مخاطره است. پیوست ب شامل مقایسه‌ای از این اصطلاحات است. استاندارد ISO/IEC 27001 شامل واپایش‌هایی است که می‌تواند برای مدیریت کردن منابع امنیتی در الف-۱۵ استفاده شود.

در مقابل، در استاندارد ISO/IEC 20000-1، طرف‌های دیگر ساختارهایی هستند که تحت واپایش مستقیم فراهم‌ساز خدمت نیستند، اما چیزی که به خدمات کمک می‌کند در دامنه کاربرد SMS است. طرف‌های دیگر می‌توانند تامین کنندگان، گروه‌های داخلی مشتریان باشند. طرف‌ها می‌توانند به قسمت بزرگی از

خدمات کمک کنند، به استاندارد ISO/IEC 20000-1:2011 بند ۴-۲ مراجعه شود. استاندارد ISO/IEC 20000-1:2011 در بند ۶-۶ الزاماتی را برای مدیریت امنیت اطلاعات مشخص می‌کند. این موضوع شامل مدیریت مخاطرات متناظر با تامین کننده می‌شود که می‌تواند به‌صورت مستقیم بر امنیت اطلاعات سازمان مشتری تاثیر بگذارد. بند ۸-۱ در استاندارد ISO/IEC 20000-1:2011 نیز به فرایند رخداد و مدیریت درخواست خدمات برای مدیریت رخدادهای امنیت اطلاعات و ارزیابی تمامی تغییرات برای بازبینی تاثیر آن بر واپایش‌های امنیت اطلاعات اشاره دارد.

هنگام طراحی کردن سامانه یکپارچه مدیریت، دو ملاحظه کلی وجود دارد که بر مدیریت روابط کسب‌وکار و فرایندهای مدیریت تامین کننده با توجه به مدیریت کردن مخاطرات طرف سوم تاثیر می‌گذارند. دو ملاحظه‌ی در زیر در نظر گرفته شده‌اند:

الف- توصیه می‌شود الزامات قراردادی امنیت اطلاعات ورودی‌ای برای فرایند ارزیابی مخاطره باشد. توصیه می‌شود این فرایند به تکمیل الزامات استاندارد ISO/IEC 20000-1 برای فراهم کنندگان خدمت کمک کند تا به نیازهای کسب‌وکاری پاسخ داده شود.

توصیه می‌شود امنیت اطلاعات در زمان مواجهه با دیگر طرف‌ها، شامل مشتریان پوشش داده شود. توصیه می‌شود این موضوع در زمانی که خدمات جدید یا تغییریافته طراحی شده‌اند و کالانما[1] خدمات و SLA ها تعریف و پذیرفته شده‌اند، در نظر گرفته شود.

دیگر مفاهیمی که در ۷-۱ در استاندارد ISO/IEC 20000-1:2011 پوشش داده شده است، مانند بازبینی‌های پیاده‌سازیی، تغییرات خدمات، مدیریت رضایتمندی مشتری و ساماندهی، می‌تواند به سامانه یکپارچه مدیریت برای مقاوم کردن کلی آن اعمال شود.

به طور خلاصه، توصیه می‌شود از رویکرد سامانه یکپارچه مدیریت استاندارد ISO/IEC 27001 برای مدیریت کردن روابط با تامین کنندگان پیروی شود؛ اما می‌تواند با الزامات مشخص شده در استاندارد ISO/IEC 20000-1:2011,6-6-6 مطابقت داشته باشد. جاییکه دارایی‌های سازمان درون دامنه کاربرد ISMS هستند اما بعضی یا تمامی آن دارایی‌ها توسط طرف دیگری واپایش شده‌اند، توصیه می‌شود سازمان قراردادهای مناسب، SLA ها یا دیگر قراردادهای مستند را بپذیرد. توصیه می‌شود این رویکرد اطمینان دهد که طرف دیگر واپایش‌های مناسب را به‌کار می‌برد.

۶-۳-۶ مدیریت تداوم و در دسترس بودن

استاندارد ISO/IEC 20000-1:2011 در بند ۶-۳ به‌صورت روشن قسمتی از حوزه امنیت اطلاعات را پوشش می‌دهد. توصیه می‌شود اقدامات مدیریت تداوم و در دسترس بودن درون سامانه مدیریت موجود، به این منظور بازبینی شوند تا امکان کارآیی آن‌ها برای پوشش دادن مدیریت یکپارچگی و محرمانگی و لذا مدیریت امنیت اطلاعات برای هر خدماتی مشاهده شود. در اینجا، جزئیات می‌تواند از استاندارد ISO/IEC 20000-1

1 - Catalouge

و اصول کلی استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴ بند الف-۱۷-۲ دریافت شود.

۶-۳-۷ مدیریت تامین کننده

استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، مدیریت تامین کننده را در الف-۱۵ پوشش می‌دهد. همچنین مراجع و پیمانکاران را در تعداد زیادی از بندها به‌کار می‌گیرد؛ به طور مثال، الف-۷-۲ و الف-۱۵-۲ و الف-۱۶-۱-۳. استاندارد ISO/IEC 20000-1:2011 بند ۴-۲ شامل الزاماتی برای هدایت فرایندهای عمل شده توسط طرف‌های دیگر و 7-2 شامل الزاماتی برای مدیریت تامین کننده است. مدیریت تامین کننده تحت هر دو استاندارد می‌تواند به‌صورت موثر ترکیب شده باشد.

۶-۳-۵ شامل اطلاعات بیشتری از مدیریت مخاطرات متناظر با مشتریان است. برای مثال، ارزیابی مخاطره استاندارد ISO/IEC 20000-1 می‌تواند گسترش یابد (با استفاده از مفاهیم استاندارد ISO/IEC 27001) تا در نظر بگیرد که آیا امنیت سازمان در برگیرنده‌ی افزودن یا کاستن تامین کننده یا تبدیل ویژه‌ی خدمات است یا نه.

توصیه می‌شود این موضوع در نظر گرفته شود حتی اگر سازمان تصمیم به نشانی دادن الزامات هر یک از استانداردها بگیرد.

۶-۳-۸ مدیریت پیکربندی

فهرست دارایی در بند الف-۸-۱-۱ در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، مخزنی از هرچیزی است که برای سازمان ارزشمند است و در دامنه کاربرد ISMS است، به طور مثال، اطلاعات، دادگان یا فرایندها.

مفهوم دادگان مدیریت پیکربندی (CMDB) در استاندارد ISO/IEC 20000-1شبیه به فهرست دارایی در استاندارد ISO/IEC 27001 است اما دامنه‌های کاربرد و لذا دورنماها متفاوت‌اند. پیاده‌سازی دامنه کاربرد در بند ۴-۵-۱ در استاندارد ISO/IEC 20000-1:2011 مورد بررسی قرار گرفته است.

الزامات در استاندارد ISO/IEC 20000-1:2011,9-1 می‌تواند در خلق کردن مدیریت ISMS استفاده شود. از دورنمای استاندارد ISO/IEC 27001، توصیه می‌شود سازمان امنیت CMDB را مدیریت کند، همان‌طور توصیه می‌شود CMDB به‌صورت دارایی در نظر گرفته شود.

استاندارد ISO/IEC 20000-1 بین سطوح مختلف یکپارچگی، انفصالی را نشان نمی‌دهد. استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، می‌تواند ارزش را بیفزاید، همان‌طور ۶-۱ نیاز دارد که مخاطرات سامانه، خدمات و عضو خدماتی ارزیابی شود و سطوح مخاطره تعیین کردند. مساله ی اولیه این است که آیا سطح مخاطره می‌تواند تغییر کند و اگر می‌تواند آیا این تغییر، مخاطره‌ای در سطح غیرقابل انتظار ایجاد می‌کند. بند ۶-۲ در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، الزام کرده است که اهداف امنیت اطلاعات باید تعریف و کسب شده باشند. توصیه می‌شود این اهداف شامل تعریف سطح قابل قبول مخاطره برای در دسترس بودن،

یکپارچگی و محرمانگی اطلاعات درون دامنه کاربرد ISMS باشند.

الزامات برای پیکربندی مبنا و رونوشت‌های اصلی مشخص شده در استاندارد ISO/IEC 20000-1 به صورت واقعی ازدیدگاه استاندارد ISO/IEC 27001 واپایش شده‌اند. توصیه می‌شود این الزامات در زمان رویکردهای یکپارچه کننده‌ی مدیریت مخاطره در نظر گرفته شوند. بعضی از این‌ها بر تصمیماتی تاثیر می‌گذارند که بر پیاده‌سازی واپایش‌ها قطعی پیاده‌سازیی موثرند.

۹-۳-۶ مدیریت انتشار و استقرار

مطابقت الزامات برای مدیریت انتشار و استقرار مشخص شده در استاندارد ISO/IEC 20000-1:2011 بند ۹-۳، تطابق با الزامات استاندارد ISO/EC 27001:2013 برای امنیت در فرایندهای توسعه‌ای و پشتیبانی را اطمینان نمی‌بخشد. مسائل امنیتی می‌تواند به‌صورت تصادفی در مدت این مرحله مشخص شود، اگر الزامات استاندارد ISO/IEC 27001 پیروی نشده باشند. مثال‌ها شامل موارد زیرند:

الف- تغییرات می‌توانند برای عملیات سامانه‌های برقرار ایجاد شده باشند که نقص‌های امنیت اطلاعات را معرفی می‌کند اگر انتشار و استقرار مدیریت امکان اقدامات بدخواهانه را در نظر نگیرد.

ب- آزمون مدیریت و محیط زنده اغلب توسط گروه‌های متفاوتی انجام می‌شود، لذا توصیه می‌شود فرایند مدیریت انتشار و استقرار این اطمینان را بدهد که نقش تولیدات صحیح داده‌ها را از گروه آزمون دریافت کند تا از مخاطرات برای داده‌های محرمانه جلوگیری کند.

این موضوع در مدت انتشارهای محرمانه به‌صورت ویژه دارای اهمیت است. در این موقعیت‌ها، روندهای مدیریت استقرار و استخدام فرارهای ممکن و متفاوت به دلیل قیود زمانی و /یا منابع می‌توانند استفاده شود. مخاطرات در بردارنده ی امنیت اطلاعات می‌توانند افزایش یافته شوند. توصیه می‌شود مخاطرات امنیت اطلاعات به‌صورت مناسب توسط فرایندهای امنیت اطلاعات پذیرفته شده مدیریت شوند؛ صرف نظر از روند مدیریت استقرار و انتشار استفاده شده.

مدیریت استقرار و انتشار می‌تواند در انتخاب واپایش‌ها در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، بند الف-۱۲-۱-۴ و الف-۱۲-۲-۹ بهبود داده شود.

پیوست الف

(آگاهی‌دهنده)

مطابقت بین استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1

الف-۱ کلیات

این پیوست مقایسهٔ محتوا در سطحِ بند بین استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 ارائه می‌دهد.

بندهایی که در آن‌ها بین استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1 در بیشتر الزامات و جزئیات اشتراکاتی وجود دارد، به‌صورت رنگ خاکستری روشن مشخص شده‌اند.

بندهایی که در آن‌ها بین پیوست الف در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴ و استاندارد ISO/IEC 20000-1 در بیشتر الزامات و جزئیات مشترکاتی وجود دارد، به رنگ خاکستری تیره مشخص شده‌اند.

نواحی بدون رنگ آن‌هایی هستند که هیچ اشتراک چشمگیری در آن‌ها وجود ندارد.

جدول الف-۱ – تناظر بین استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1

برمبنای مقایسهٔ SC27 ISO.IEC 27001	برمبنای مقایسهٔ SC20 استاندارد ISO/IEC20000-1
(هنوز) الزاماتی وجود ندارد لذا به حساب آورده نمی‌شود	مقدمه
(هنوز) الزاماتی وجود ندارد لذا به حساب آورده نمی‌شود	۱ هدف و دامنه کاربرد
(هنوز) الزاماتی وجود ندارد لذا به حساب آورده نمی‌شود	۱-۱ کلیات
(هنوز) الزاماتی وجود ندارد لذا به حساب آورده نمی‌شود	۱-۲ کاربرد
۲ مراجع الزامی	۲ مراجع الزامی
۳ اصطلاحات و تعاریف	۳ اصطلاحات و تعاریف
۴ بافت سازمان	بسیار- به قسمت زیر مراجعه شود
۴-۱ درک سازمان و بافت آن	۴-۱-۱ مدیریت تعهدات
۴-۲ درک نیازها و انتظارات طرف‌های علاقه-مند	۵-۲ پاراگراف ۱، طرح‌ریزی خدمات جدید یا تغییریافته ۵-۴ پاراگراف ۱، انتقال خدمات جدید یا تغییریافته

برمبنای مقایسهٔ SC27 ISO.IEC 27001	برمبنای مقایسهٔ SC20 استاندارد ISO/IEC20000-1
	۶-۲ پاراگراف ۱، گزارش خدمات ۶-۳-۱ پاراگراف ۱، تداوم خدمات و الزامات قابلیت دسترسی ۶-۵ پاراگراف ۱، مدیریت توانایی ۷-۱ پاراگراف ۱و ۳-مدیریت روابط کسب‌وکار ۸-۱ پاراگراف ۵، مدیریت تقاضای رخداد و خدمات ۹-۲ پاراگراف ۸ و ۱۰، پاراگراف یکی مانده به آخر، مدیریت تغییر ۹-۳ پاراگراف ۲ و ۵، مدیریت واگذاری و آرایش
۴-۳ تعیین محدوده سیستم مدیریت امنیت اطلاعات	۴-۲-۱ کاربست پذیری ۴-۲ نظارت فرایندها عمل شده توسط طرف‌های دیگر ۴-۳ مدیریت سندسازی ۴-۵-۱ تعریف دامنه کاربرد ۴-۵-۲ طرح‌ریزی SMS (همچنین به استاندارد ISO/IEC 20000-3 مراجعه شود)
۴-۴ سیستم مدیریت امنیت اطلاعات	برابری مستقیمی وجود ندارد
۵ رهبری	۴-۱ مسئولیت مدیریت
۵-۱ رهبری و تعهد	۴-۱-۱ تعهدات مدیریت
۵-۱ الف- رهبری و تعهدات	۴-۱-۱-الف تعهدات مدیریت
۵-۱ ب- رهبری و تعهدات	۴-۱-۱-ب تعهدات مدیریت ۴-۲ نظارت فرایندهای انجام شده توسط طرف‌های دیگر ۷-۲ مدیریت روابط کسب‌وکاری
۵-۱ پ- رهبری و تعهدات	۴-۱-۱- ث تعهدات مدیریت ۴-۴-۱ پاراگراف ۱، تدارکات منابع ۴-۵-۲ چ– طرح‌ریزی SMS ۴-۵-۴-۳-پ- بازبینی مدیریت ۵-۲-ت – طرح‌ریزی خدمات جدید یا تغییریافته ۵-۳-پ- طراحی و توسعهٔ خدمات جدید یا تغییریافته ۶-۴-الف- ۱)۲) بودجه‌ریزی و حساب داری خدمات ۶-۵- پ ۲. مدیریت ظرفیت
۵-۱ ت- رهبری و تعهدات	۴-۱-۱ تعهدات مدیریت ۴-۱-۲-خط‌مشی مدیریت خدمت
۵-۱ ث- رهبری و تعهدات	۴-۱-۱-ب- تعهدات مدیریت
۵-۱ ج- رهبری و تعهدات	۴-۱-۱ تعهدات مدیریت ۴-۱-۳-صلاحیت، مسئولیت و ارتباطات
۵-۱ چ- رهبری و تعهدات	۴-۱-۲-پ- خط‌مشی مدیریت خدمت
۵-۱ ح- رهبری و تعهدات	۴-۱-۳-۱-۴-۳-صلاحیت، مسئولیت و ارتباطات

برمبنای مقایسهٔ SC27 ISO.IEC 27001	برمبنای مقایسهٔ SC20 استاندارد ISO/IEC20000-1
۵-۲ خط‌مشی	۴-۱-۱-الف)ب) تعهدات مدیریت ۴-۱-۲-خط‌مشی مدیریت خدمت ۴-۳-۱- احراز کردن و نگهداشت اسناد ۴-۳-۳-نگهداشت مدارک
۵-۳ نقش‌ها، مسئولیت‌ها و اختیارات سازمانی	۴-۱-۳- صلاحیت، مسئولیت و ارتباطات ۴-۱-۴- نماینده‌ی مدیریت ۴-۳-۳-واپایش‌های ثبت‌ها ۴-۴-۵-۲ ممیزی اینترنت
۶ طرح‌ریزی	۴-۵-۲ طرح‌ریزی SMS
۶-۱ اقدامات برای پرداختن به مخاطرات و فرصت‌ها	قسمت زیر مشاهده شود
۶-۱-۱ اقدامات برای پرداختن به مخاطرات و فرصت‌های عمومی	منابع مخاطره: ۴-۵-۲-د) طرح‌ریزی SMS ۴-۵-۳-ت) پیاده‌سازی و عملیات SMS ۴-۵-۴-۳-ث) بازبینی مدیریت ۴-۵-۵-۲-الف) بهبودهای مدیریت ۵-۳-طراحی و توسعهٔ خدمات جدید یا تغییریافته ۵-۲-ج-طراحی خدمات جدید یا تغییریافته ۶-۳-۱- پ ۱. تداوم خدمات و در دسترس بودن ی خدمات ۶-۶-۱-پ) خط‌مشی امنیت اطلاعات ۶-۶-۳-الف) تغییرات و رخدادهای امنیت اطلاعات ۸-۲-مدیریت مساله ۹-۲- پ ۸. مدیریت تغییر
۶-۱-۲ ارزیابی مخاطرات امنیت اطلاعات	بند ۶-۶ در استاندارد ISO/IEC 20000-1معادل آن است اما منابع مخاطره‌ی بسیاری با الزامات مشابه وجود دارند: ۴-۵-۲-د) طرح‌ریزی SMS ۵-۵-۳-ت) پیاده‌سازی و عملیات SMS ۴-۵-۳-ث) بازبینی مدیریت ۵-۲-ج) طرح‌ریزی خدمات جدید یا تغییریافته ۶-۳-۱- پ ۱. تداوم خدمات و در دسترس بودن ی الزامات ۶-۶-۱-پ) , ت) خط‌مشی امنیت اطلاعات ۶-۶-۳-الف) پ ۲. تغییرات و رخدادهای امنیت اطلاعات ۹-۲- پ ۸. مدیریت تغییرات
۶-۱-۳ برطرف‌سازی مخاطرات امنیت اطلاعات	به‌استثنای بند ۶-۶، مطابقت مستقیمی با استاندارد ISO/IEC 20000-1 وجود ندارد، اما منابع بسیاری برای مخاطره با الزامات مشابه وجود دارند.

برمبنای مقایسهٔ SC27 ISO.IEC 27001	برمبنای مقایسهٔ SC20 استاندارد ISO/IEC20000-1
	۴-۱-۱-چ) تعهدات مدیریت ۴-۳-۱- احراز کردن و نگهداشت اسناد ۴-۵-۲-د- طرح‌ریزی SMS ۴-۵-۳-ت – پیاده‌سازی و عملیات SMS ۵-۲-ج–طرح‌ریزی خدمات جدید و تغییریافته ۶-۶-۲-ت) پ ۲. واپایش‌های امنیت اطلاعات
۶-۲ اهداف امنیت اطلاعات و طرح‌ها برای دستیابی به آن‌ها	۴-۱-۱ تعهدات مدیریت
۷-۱ منابع	۴-۱-۱-ث) مدیریت تعهدات ۴-۴- مدیریت منابع
۷-۲ شایستگی	۴-۳ مدیریت مستندات -۴-۲- منابع انسانی
۷-۳ آگاه‌سازی	۴-۱ مسئولیت مدیریت ۴-۴-۲ ت) منابع انسانی
۷-۴ ارتباطات	۴-۱-۱-الف)پ)ت) مسئولیت مدیریت ۴-۱-۳-ب) صلاحیت، مسئولیت و ارتباطات ۴-۳-۲-ب) واپایش سند ۴-۵-۴-۱- پ آخر، کلیات ۵-۵-۴-۲-پ آخر، ممیزی داخلی ۵-۲-پ) طرح‌ریزی خدمات جدید یا تغییریافته ۶-۲- پ آخر، گزارش خدمات ۶-۶-۱-الف) خط‌مشی امنیت اطلاعات ۷-۱-پ ۳، مدیریت روابط کسب‌وکار ۷-۲-د) مدیریت تامین کننده ۹-۲-پ ۱۰، مدیریت تغییرات
۷-۵ اطلاعات مستند	۴-۳- مدیریت مستندسازی
۷-۵-۱ کلیات	۴-۳-۱- سندهای استقرار و نگهداشت
۷-۵-۲ ایجاد و به‌روزرسانی	۴-۳-۲- واپایش سند ۴-۳-۳-واپایش ثبت‌ها
۷-۵-۳ کنترل اطلاعات مستند	۴-۳-۲ واپایش سند ۴-۳-۳ واپایش ثبت‌ها
۸ عملیات	۴-۵ انتشار و بهبود SMS (بند ۵ تا ۹)
۸-۱ طرح‌ریزی و واپایش عملیات	۴-۲ هدایت فرایندهای عمل شده توسط طرف‌های دیگر ۴-۵ انتشار و بهبود SMS بسیاری از نکات در بند ۶ تا ۱۹ هستند.

برمبنای مقایسهٔ SC27 ISO.IEC 27001	برمبنای مقایسهٔ SC20 استاندارد ISO/IEC20000-1
۸-۲ ارزیابی مخاطرات امنیت اطلاعات	هیچ معادل مستقیمی در استاندارد ISO/IEC 20000-1وجود ندارد، به‌استثنای بند ۶-۶، اما مراجع بسیاری با مخاطره با الزامات مشابه ۴-۵-۲-د) طرح‌ریزی SMS ۴-۵-۳-ت)پیاده‌سازی و عملیات SMS ۴-۵-۴-۳-ث) بازبینی مدیریت ۵-۲-ج) طرح‌ریزی خدمات جدید یا تغییر کرده ۶-۳-۱-پ ۱، الزامات تداوم خدمات و در دسترس بودن ۶-۶-۱-پ), ت) خط‌مشی امنیت اطلاعات ۶-۶-۳- الف) پ ۲، تغییرات و رخدادهای امنیت اطلاعات ۹-۲-پ ۸، مدیریت تغییرات
۸-۳ برطرف‌سازی مخاطرات امنیت اطلاعات	در استاندارد ISO/IEC 20000-1 معادل مستقیمی وجود ندارد، به‌جز برای بند ۶-۶، اما مراجع زیادی با مخاطره‌ی الزامات مشابه وجود دارد، ۴-۱-۱-چ) تعهدات مدیریت ۴-۳-۱ سند انتشار و نگهداشت ۴-۵-۲-د طرح‌ریزی SMS ۴-۵-۳- ت) پیاده‌سازی و عملیات SMS ۵-۲- f) طرح‌ریزی خدمات جدید و تغییریافته ۶-۶-۲- d) پ ۲، واپایش‌های امنیت اطلاعات
۹ ارزشیابی عملکرد	به قسمت زیر مراجعه شود
۹-۱ پایش، اندازه‌گیری، تحلیل و ارزشیابی	۴-۱-۱الف)ت)ج) خط‌مشی مدیریت خدمت ۴-۳-۳- پ ۱، واپایش ثبت‌ها ۴-۵-۳-ج) پیاده‌سازی و عملیات SMS ۴-۵-۴ کلیات ۶-۲ گزارش خدمات ۸-۲ مدیریت مساله
۹-۲ ممیزی داخلی	۴-۵-۴-۲ ممیزی داخلی ۴-۳-۱ اسناد انتشار و نگهداشت ۴-۳-۳ واپایش ثبت‌ها
۹-۳ بازنگری مدیریت	۴-۱-۲-پ) خط‌مشی مدیریت خدمت ۴-۳-۳ واپایش‌های ثبت ۴-۵-۴-۳ بازبینی مدیریت
۱۰ بهبود	۴-۵-۵ نگهداری و بهبود SMS
۱۰-۱ عدم انطباق و اقدام اصلاحی	۴-۱-۲-پ) خط‌مشی مدیریت خدمت ۴-۳-۱ انتشار و نگهداشت سند ۴-۳-۳ واپایش ثبت‌ها ۴-۵-۴ پایش و بازبینی SMS

برمبنای مقایسهٔ SC27 ISO.IEC 27001	برمبنای مقایسهٔ SC20 استاندارد ISO/IEC20000-1
	۴-۵-۵ نگهداشت و بهبود SMS ۸-۲ مدیریت مساله
۱۰-۲ بهبود مستمر	۴-۱-۲-پ) خطمشی مدیریت خدمت ۴-۵-۵-نگهداشت و بهبود SMS ۹-۲- پ آخر، مدیریت تغییرات
الف-۵ خطمشی‌های امنیت اطلاعات	به قسمت زیر مراجعه شود
الف-۵-۱ جهت‌گیری مدیریت برای امنیت اطلاعات	۶-۶-۱- خطمشی امنیت اطلاعات
الف-۶ سازمان امنیت اطلاعات	به قسمت زیر مراجعه شود
الف-۶-۱ سازمان داخلی	در 20000-1 مشخص نشده است
الف-۶-۲ افزاره‌های سیار و دورکاری	در 20000-1 مشخص نشده است
الف-۷ امنیت منابع انسانی	به قسمت زیر مراجعه شود
الف-۷-۱ پیش از اشتغال	در 20000-1 مشخص نشده است
الف-۷-۲ در حین خدمت	۶-۶-۱ خطمشی امنیت اطلاعات
الف-۷-۳ خاتمه و تغییر اشتغال	در 20000-1 مشخص نشده است
الف-۸ مدیریت دارایی	به قسمت زیر مراجعه شود
الف-۸-۱ مسئولیت دارایی‌ها	۶-۶-۲ واپایش‌های امنیت اطلاعات
الف-۸-۲ طبقه‌بندی اطلاعات	در 20000-1 مشخص نشده است
الف-۸-۳ اداره‌کردن رسانه‌های ذخیره‌سازی	در 20000-1 مشخص نشده است
الف-۹ واپایش دسترسی	به قسمت زیر مراجعه شود
الف-۹-۱ الزامات کسب‌وکار واپایش دسترسی	در 20000-1 مشخص نشده است
الف-۹-۲ مدیریت دسترسی کاربر	در 20000-1 مشخص نشده است
الف-۹-۳ مسئولیت‌های کاربر	در 20000-1 مشخص نشده است
الف-۹-۴ واپایش دسترسی به برنامه‌های کاربردی و سامانه‌ها	در 20000-1 مشخص نشده است
الف-۱۰ رمزنگاری	به قسمت زیر مراجعه شود
الف-۱۰-۱ واپایش‌های رمزنگاری	در 20000-1 مشخص نشده است
الف-۱۱ امنیت فیزیکی و محیطی	به قسمت زیر مراجعه شود
الف-۱۱-۱ نواحی امن	در 20000-1 مشخص نشده است
الف-۱۱-۲ تجهیزات	در 20000-1 مشخص نشده است
الف-۱۲ امنیت عملیات	به قسمت زیر مراجعه شود
الف-۱۲-۱ مسئولیت‌ها و روش‌های اجرایی عملیاتی	در 20000-1 مشخص نشده است
الف-۱۲-۲ حافظت در برابر بدافزار	در 20000-1 مشخص نشده است
الف-۱۲-۳ نسخه‌های پشتیبان	۶-۳ مدیریت تداوم خدمات و در دسترس بودن

برمبنای مقایسهٔ SC27 ISO.IEC 27001	برمبنای مقایسهٔ SC20 استاندارد ISO/IEC20000-1
الف-۱۲-۴ واقعه‌نگاری و پایش	در 20000-1 مشخص نشده است
الف-۱۲-۵ واپایش نرم‌افزار عملیاتی	در 20000-1 مشخص نشده است
الف-۱۲-۶ مدیریت آسیب‌پذیری فنی	در 20000-1 مشخص نشده است
الف-۱۲-۷ ملاحظات ممیزی سامانه مدیریت	در 20000-1 مشخص نشده است
الف-۱۳ امنیت ارتباطات	به قسمت زیر مراجعه شود.
الف-۱۳-۱ مدیریت امنیت شبکه	در 20000-1 مشخص نشده است
الف-۱۳-۲ انتقال اطلاعات	در 20000-1 مشخص نشده است
الف-۱۴ مالکیت، توسعه و نگهداشت سامانه	به قسمت زیر مراجعه شود.
الف-۱۴-۱ الزامات امنیتی سامانه‌های اطلاعاتی	۶-۶-۳ تغییرات و رخداد امنیت اطلاعات
الف-۱۴-۲ امنیت در فرایند توسعه و پشتیبانی	۶-۶-۳ تغییرات و رخداد امنیت اطلاعات
الف-۱۴-۳ آزمون داده	در 20000-1 مشخص نشده است
الف-۱۵روابط تامین کنندگان	به قسمت زیر مراجعه شود.
الف-۱۵-۱ امنیت اطلاعات در روابط تامین کنندگان	۶-۶-۲ واپایش‌های امنیت اطلاعات
الف-۱۵-۲ مدیریت تحویل خدمات تامین کننده	۲-۴ هدایت فرایندهای عمل شده توسط طرف‌های دیگر ۲-۷ مدیریت تامین کننده
الف-۱۶ مدیریت رخداد امنیت اطلاعات	به قسمت زیر مراجعه شود.
الف-۱۶-۱ مدیریت رخداد امنیت اطلاعات و بهبودها	۶-۶-۳ تغییرات و رخدادهای امنیت اطلاعات ۸-۱ مدیریت رخداد و درخواست خدمات
الف-۱۷ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار	به قسمت زیر مراجعه شود.
الف-۱۷-۱ تداوم امنیت اطلاعات	در 20000-1 مشخص نشده است
الف-۱۷-۲ تکرار اطلاعات	۶-۳ مدیریت در دسترس بودن و تداوم خدمت
الف-۱۸ مطلوبیت	به قسمت زیر مراجعه شود.
الف-۱۸-۱ مطلوبیت با الزامات قانونی و قراردادی	۶-۶-۱ خط‌مشی امنیت اطلاعات
الف-۱۸-۲ بازبینی‌ها امنیت اطلاعات	۶-۶-۱ خط‌مشی امنیت اطلاعات ۶-۶-۲ واپایش‌های امنیت اطلاعات ۶-۶-۳ تغییرات و رخدادهای امنیت اطلاعات

پیوست ب

(آگاهی‌دهنده)

مقایسه اصطلاحات استانداردهای ISO/IEC 27000 و ISO/IEC 20000-1

ب-۱ کلیات

در جدول ب-۱، به منظور اختصار، به استانداردها بدون سال انتشار در ستون «توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد» اشاره شده است. جدول ب-۱ مقایسه‌ای از اصطلاحات تعریف شده در استاندارد ISO/IEC 27000 (که واژه‌نامه‌ای برای استاندارد ISO/IEC 27001) اصطلاحات استفاده شده در استاندارد ISO/IEC 27001 و اصطلاحات تعریف شده یا استفاده شده در استاندارد ISO/IEC 20000-1 فراهم می‌کند. نواحی‌ای که در آن اصطلاحات به‌صورت متفاوت بین استاندارد ISO/IEC 27000 و استاندارد ISO/IEC 20000-1 تعریف شده‌اند به‌صورت خاکستری روشن مشخص شده‌اند.

جدول ب-۱- مقایسه اصطلاحات

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
واپایش(کنترل) دسترسی	۲-۱ حصول اطمینان از اینکه دسترسی به دارایی‌ها به‌صورت مجاز و محدود بر اساس الزامات امنیتی و الزامات کسب‌وکار است.	تعریف نشده	فاقد معادل مستقیم
حمله	۲-۳ تلاش برای تخریب، افشا، دست‌کاری، از کار انداختن، سرقت یا دسترسی غیرمجاز یا استفاده غیرمجاز از دارایی است.	تعریف نشده	فاقد معادل مستقیم
ممیزی	۲-۵ فرایندی نظام‌مند، مستقل و مستند برای کسب و ارزشیابی هدفمند شواهد عینی ممیزی، به منظور تعیین میزان برآورده شدن معیارهای ممیزی است. **یادآوری ۱-** ممیزی می‌تواند،	تعریف نشده	به‌صورت وسیع در دو استاندارد به یک معنا است.

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
	ممیزی داخلی (طرف اول) یا خارجی (طرف دوم یا سوم) باشد و همچنین می‌تواند ممیزی ترکیبی باشد (ترکیبی از دو یا چندین نظام) **یادآوری ۲**- «شواهد ممیزی» و «معیارهای ممیزی» در استاندارد ISO 19011 تعریف شده است.		
اصالت‌سنجی	۷-۲ کسب اطمینان از آنکه مشخصهٔ ادعاشده هستار[1]، درست است.	تعریف نشده	ارتباط مستقیمی به این اصطلاح مربوط به امنیت اطلاعات نیست «اصالت‌سنجی»: که در استاندارد ISO/IEC 27001 به‌صورت فنی تعریف شده است. «اصالت‌سنجی» در اقدامات چرخه‌ی زندگی سامانه مدیریت شبیه به «درستی سنجی» نیست.
اصالت	۸-۲ خصوصیتی که یک هستار، همان است که ادعا می‌کند.	۱۱-۳ **یادآوری ۱**- دیگر خصوصیات مانند اصالت‌سنجی، پاسخگویی، رد نکردن و اطمینان‌پذیری نیز می‌توانند درگیر شوند.	با ارجاع به استاندارد ISO/EC 20000-1، اما بعد از آن استفاده نشده است.
در دسترس بودن	۹-۲ خصوصیت دسترسی‌پذیر و قابل‌استفاده بودن، به‌محض تقاضای یک هستار مجاز است.	۱-۳ توانایی مسئول خدمات برای پیاده‌سازی آن کارکرد مورد نیاز در زمان مورد پذیرش یا در دوره‌ی زمانی مقبول **یادآوری**- در دسترس بودن به‌صورت متداول به‌صورت نسبت یا درصد زمانی بیان می‌شود که خدمات برای استفاده توسط مشتری در زمانی که توصیه می‌شود خدمت در دسترس بودن باشد در دسترس است. ۱۱-۳ **یادآوری ۱**- علاوه بر این، دیگر خصوصیات مانند اصالت‌سنجی، جوابگویی، اطمینان‌پذیری می‌تواند درگیر باشد. **یادآوری ۲**- اصطلاح «در	«به امنیت اطلاعات مراجعه شود» در دسترس بودن اغلب مرکزی برای مدیریت خدمت در نظر گرفته می‌شود و نقشی مهم در استاندارد ISO/IEC 20000-1 در جنبه‌های ارزیابی کیفیت خدامت فراهم شده بازی می‌کند. به بند ۶-۳ از استاندارد ISO/IEC 20000-1 مراجعه شود. تفاوت بین دو تعریف زیاد نیست اما به دلیل اهمیت «دسترسی‌پذیری» در مدیریت خدمت، این تفاوت ارزشمند است. نتیجه‌ی حاصل از تفاوت بین دو معنای در دسترس بودن این است که تعریف استاندارد ISO/IEC 27000 از امنیت اطلاعات برای استاندارد ISO/IEC 20000-1 توسط استفاده از در دسترس بودن به جای در دسترس بودن پذیرفته شده بود.

[1] - Entity

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		دسترس بودن» در این تعریف استفاده نشده است زیرا اصطلاح تعریف شده‌ای در این قسمت از استاندارد ISO/IEC 20000 است که برای این تعریف مناسب نیست. **یادآوری ۳**- از استاندارد ISO/IEC 27000 اقتباس شده است.	
محرمانگی	۲-۱۲ خصوصیتی که اطلاعات برای افراد، هستارها یا فرایندهای (۲-۶۱) غیرمجاز در دسترس نبوده یا افشا نشود.	تعریف نشده	فاقد معادل مستقیم
پیکربندی مبنا	تعریف نشده	۳-۲ پیکربندی مبنا اطلاعات به‌صورت رسمی در زمانی مشخص رد مدت زندگی خدمات اختصاص یافته است. **یادآوری ۱**- پیکربندی بعلاوه ی تغییرات پذیرفته شده از مبناها، پیکربندی اخیر اطلاعات را تشکیلی می‌دهد. **یادآوری ۲**- از استاندارد ISO/IEC/IEEE 24765:2010 اقتباس شده است.	اصطلاح استفاده شده در بند استاندارد ISO/IEC 20000-1 به این صورت است: «... پیکربندی مبنای CI های تاثیر یافته باید پیش از به‌کارگیری رهایی به محیط زندگی گرفته شود.»
قلمِ پیکربندی	تعریف نشده	۳-۳ عنصری که نیاز است به منظور تحویل خدمات واپایش شود.	CI ها در استاندارد ISO/IEC 20000-1 مهم هستند و مولفه ای از خدمات در نظر گرفته می‌شوند. CI ها می‌توانند یکی یا قسمتی از مولفه ی خدماتی باشند. دارایی اطلاعاتی می‌تواند CI باشد. به تعریف ۳-۲۷ مولفه خدمات در استاندارد ISO/IEC 20000-1 مراجعه شود.
دادگان مدیریت پیکربندی (CMDB)	تعریف نشده	۳-۴ ذخیره‌سازی داده برای ثبت نمودن خواص CI ها و رابطه‌ی بین CIها در	وابسته به روش پذیرفته شده توسط سازمان، CMDB می‌تواند برای نگهداری فهرست دارای ها استفاده شود. به استاندارد ISO/IEC 27001 قسمت پیوست الف و

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		چرخه‌ی زندگی آن‌ها استفاده می‌شود	بند الف-۷-۱-۱ مراجعه شود.
بهبود مستمر	تعریف نشده	۵-۳ فعالیتی بازگشتی به منظور توانایی در برآوردن الزامات خدمت. **یادآوری**- از استاندارد ISO/IEC 9000:2005 اقتباس شده است.	بند 2-1-4 در استاندارد ISO/IEC 20000-1 نیازمند خط‌مشی برای بهبود پیوسته که قسمتی از خط‌مشی مدیریت خدمت می‌باشد، است. چرخه‌ی PDCA در بسیاری از موارد شبیه به ISO 9001 و ISO.IEC20000-1 (به طور مثال استاندارد ISO/IEC 27001 در بند ۴-۲-۴ و استاندارد ISO/IEC 20000-1 در بند ۴-۵-۵) است.
واپایش(کنترل)	۲-۱۶ اقدامی که مخاطره (۲-۶۸) را اصلاح می‌کند **یادآوری ۱**- واپایش‌ها می‌توانند شامل هر فرایند، خط‌مشی، افزاره، روش یا هر اقدام دیگری شود که مخاطره را اصلاح کند. **یادآوری ۲**- واپایش‌ها ممکن است همیشه منجر به اثر اصلاحی مفروض و مورد نظر نشود. (در تعریف ۳-۸-۱-۱ ISO Guide 73: 2009)	تعریف نشده	کلمه‌ی واپایش در استاندارد ISO/IEC 20000-1 هم به عنوان اسم و هم به عنوان فعل به کار رفته اما به‌صورت اصطلاحی مشخص تعریف نشده لذا معنای آن انگلیسی متداول به‌صورت زیر است: اسم: صلاحیت یا مسئولیت، قدرت تاثیر یا هدایت، واپایش کردن، ابزاری از محدودیت‌ها، (واپایش) افزاره‌ای برای عمل کردن تنظیمات یا آزمودن (ماشین؛ سامانه و...) فعل: (واپایش شده، واپایش کننده) برای داشتن یا اعمال کردن توانی بر کسی یا چیزی برای تنظیم کردن، محدود کردن یا آزمودن (ماشین، سامانه یا...) تمامی استفاده از واپایش در نقش اسم در بند ۶-۶- استاندارد ISO/IEC 20000-1 یعنی «مدیریت امنیت اطلاعات» است، استفاده دیگر در بند 2-3-4 و 3-3-4 است که تقریبا به‌صورت تحت الفظی از ISO 9001:2008 گرفته شده است. واپایش به‌صورت فعل در مکان‌های زیادی به کار رفته است، معمولا به‌صورت: «واپایش از فرایندهای XXX» یا «X باید توسط Y واپایش شود».

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
هدف واپایش	۲-۱۷ بیانیه‌ای که آنچه باید در نتیجهٔ پیاده‌سازی واپایش‌ها (۲-۱۶) به دست آید را توصیف می‌کند.	تعریف نشده	اسم «هدف»: در استاندارد ISO/IEC 20000-1 مطابق با انگلیسی متداول استفاده شده است: چیزی که برای آن تلاش می‌کنیم، هدف کمینه پیوندی دقیق بین استفاده از «هدف واپایشی» در استاندارد ISO/IEC 27001 استفاده از آن در بند ۴ استاندارد ISO/IEC 20000-1 به‌صورت «اهداف مدیریت خدمت» یا بند ۶-۶ «اهداف مدیریت امنیت اطلاعات» وجود دارد.
اصلاح	۲-۱۸ اقدامی که برای از بین بردن عدم انطباق (۲-۵۳) شناسایی‌شده انجام می‌گیرد.	تعریف نشده	فاقد معادل مستقیم
اقدام اصلاحی	۲-۱۹ اقدامی که برای از بین بردن علت عدم انطباق (۲-۵۳) و جلوگیری از تکرار آن انجام می‌شود. (ISO 9000:2005)	۳-۶ اقدامی که به منظور حذف نمودن یا کاهش احتمال وقوع مجدد عدم تطابق آشکارشده یا دیگر موقعیت‌ها نامطلوب انجام می‌شود. **یادآوری**- از استاندارد ISO/IEC 9000:2005 اقتباس شده است.	هر دو بر مبنای ISO 9000: 2005 هستند. به «اقدام ممانعت کننده» مراجعه شود.
مشتری	تعریف نشده	۳-۷ سازمان یا قسمتی از سازمان که خدماتی را دریافت می‌کند. **یادآوری ۱**- مشتری می‌تواند نسبت به سازمان فراهم‌ساز خدمت داخلی یا خارجی باشد. **یادآوری ۲**- از استاندارد ISO/IEC 9000:2005 اقتباس شده است.	در استاندارد ISO/IEC 20000-1 مشتری می‌تواند به‌صورت تامین کننده عمل کند. در استاندارد ISO/IEC 27001 مشتری طرف جلب شده است.
سند	تعریف نشده	۳-۸ اطلاعات و واسطه پشتیبانی آن (ISO 9000:2005)	فاقد معادل مستقیم

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		مثال‌ها خط‌مشی‌ها، طرح‌ها، توصیف فرایند، روندها، موافقت‌نامه‌ی سطح خدمت، تماس‌ها یا ثبت‌ها. **یادآوری ۱**- مستندسازی می‌تواند در هر قالب یا نوع باشد. **یادآوری ۲**- در استاندارد ISO/IEC 20000، مستندات به‌جز برای ثبت‌ها، مقصودی را بیان می‌کند که تمایل به کسب آن است.	
اثربخشی	۲۴-۲ میزانی که فعالیت‌های طرح-ریزی‌شده تحقق‌یافته و نتایج طرح‌ریزی‌شده به‌دست‌آمده است.	۹-۳ اندازه‌ای که اقدامات طرح‌ریزی شده در آن تحقق یافته‌اند و نتایج طرح‌ریزی شده کسب شده‌اند (ISO 9000:2005)	همانندی
رویداد	۲۵-۲ وقوع یا تغییر مجموعه‌ای ویژه از شرایط است. (ISO/IEC Guide 73:2009) **یادآوری ۱**- رویداد می‌تواند یک یا تعداد بیشتری پیشامد است و می‌تواند دلایل مختلفی داشته باشد. **یادآوری ۲**- رویداد می‌تواند شامل چیزی باشد که رخ نداده است. **یادآوری ۳**- رویداد می‌تواند بعضی اوقات به‌صورت «رخداد» یا «تصادف» اشاره کند.	تعریف نشده	کلمه‌ی رویداد در استاندارد ISO/IEC 20000-1 تعریف شده است به همان معنای خود در انگلیسی متداول: چیزی که رخ می‌دهد. برای مثال، به بند ۶-۲ در استاندارد ISO/IEC 20000-1 مراجعه شود «رویداد چشم‌گیر» یا تداوم خدمات ۶-۳-۲ و در دسترس بودن طرح‌ها: «در رویدادی با کاهش گسترده‌ی خدمات» این استفاده مشابه به استاندارد ISO/IEC 27001 است، لذا به‌صورت گسترده قابل مقایسه است. به «رویداد امنیت اطلاعات» مراجعه شود.
رخداد	به رخداد امنیت اطلاعات مراجعه شود.	۱۰-۳ قطع شدن طرح‌ریزی نشده‌ی خدمات، کاهش کیفیت خدمات یا رویداد که هنوز روی خدمت مشتری تاثیر نداشته است.	تفاوت چشم‌گیری بین استفاده از رخداد در استاندارد ISO/IEC 27001 و در استاندارد ISO/IEC 20000-1 وجود دارد. کلمه‌ی رخداد در استاندارد ISO/IEC 27001 برای اشاره به «رخداد امنیت اطلاعات» استفاده شده است. در استاندارد

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
			این کلمه دارای معنای تعریف شده به‌صورت مشخص‌تر نسبت به استاندارد ISO/IEC 27001 است. در استاندارد ISO/IEC 20000-1 «رخداد» یکی از دنباله‌های اصطلاحات مرتبط است و تنها متناظر با رخدادهای امنیت اطلاعات است. دیگر اصطلاحات مرتبط عبارت‌اند از: ۳-۱۹- مساله ریشه‌ای که سبب یک یا تعداد بیشتری رخداد است. ریشه‌ای که به صور معمول در زمانی که ثبت مساله ایجاد شده، شناخته نشده است و فرایند مدیریت مساله برای بررسی‌های بیشتر منطقی است. ۳-۱۵- خطای شناخته شده مساله ای که دارای ریشه‌ی شناخته شده است یا روشی برای کاهش یا حذف تاثیر آن بر خدمت توسط کار پیرامون آن. رخداد عمده (اصطلاح تعریف نشده) رخدادی که از نظر دسته‌بندی دارای بالاترین تاثیر است. هر «رخداد»، «مساله» و «رخداد عمده» به‌صورت متفاوت مدیریت شده‌اند و درون الزامات مختلفی قرار دارند. «خطای معلوم» مساله ای این که در آن فاعل شناخته شده و توسط فرایند مدیریت مساله؛ مدیریت شده است و شامل الزاماتی می‌شود که برای اولین بار اعلام می‌کند که مساله دارای خطای معلومی شده است. «رخداد بزرگ» توسط فرایندهای رخداد و مدیریت درخواست خدمات مدیریت شده است و الزاماتی دارد که در آن روندی برای مدیریت کردن «رخدادهای عمده» وجود دارد. به «رخداد امنیت اطلاعات» مراجعه شود.

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
امنیت اطلاعات	۲-۳۳ حفظ محرمانگی (۲-۱۲)، یکپارچگی (۲-۴۰) و در دسترس بودن (۲-۹) اطلاعات است. **یادآوری ۱-** علاوه بر این، سایر خصوصیت‌ها همچون اصالت (۲-۸)، پاسخگویی، سلب انکار (۲-۵۴) و اطمینان‌پذیری (۲-۶۲) را نیز می‌تواند دربرگیرد.	۳-۱۱ حفاظت از تطابق، یکپارچگی و دسترسی-پذیری اطلاعات. یادآوری ۱- دیگر خصوصیات مانند اصالت‌سنجی و پاسخگویی، قابلیت اطمینان می‌توانند درگیر شوند. یادآوری ۲- اصطلاح «در دسترس بودن» در این تعریف استفاده نشده است زیرا اصطلاحی تعریف شده در این قسمت از استاندارد ISO/IEC 20000 است که برای این تعریف مناسب نیست. یادآوری ۳- از استاندارد ISO/IEC 27000 اقتباس شده است.	در استاندارد ISO/IEC 20000-1 کلمه «در دسترس بودن» نمی‌تواند در تعریف امنیت اطلاعات در ۳-۱۱ استفاده شود زیرا در دسترس بودن اصطلاحی تعریف شده با معنای متفاوت است. این تعریف برای امنیت اطلاعات و به منظور استفاده از اصطلاح «دسترسی‌پذیری» است. در دسترس بودن از تعریف خصوصیت در دسترس بودن در استاندارد ISO/IEC 27000 گرفته شده است که در دسترس بودن و قابل استفاده بودن تقاضایی توسط ساختار صلاحیت‌دار است.
تداوم امنیت اطلاعات	۲-۳۴ فرایندها (۲-۶۲) و روش‌های اجرایی برای اطمینان از تداوم عملیات امنیت اطلاعات (۲-۳۳) است.	تعریف نشده	استاندارد ISO/IEC 27000 بر مفهوم عملیات نگهداشت امنیت اطلاعات در مدت رویداد تداوم کسب‌وکار به‌صورت منفصل از نگهداشت تمامی خدمات تمرکز دارد تداوم خدمات در استاندارد ISO/IEC 20000-1 به‌صورت زیرمجموعه‌ای تداوم کسب‌وکار استفاده شده است. به «تداوم خدمات» مراجعه شود.
رویداد امنیت اطلاعات	۲-۳۵ پیشامد شناسایی سامانه، خدمات یا حالت شبکه که نشان‌دهنده‌ی نقص ممکن خط‌مشی امنیت اطلاعات یا شکست واپایش‌ها یا موقعیت ناشناخته‌ای است که ممکن است مربوط به امنیت باشد	تعریف نشده	«رویداد امنیت اطلاعات» تنها در استاندارد ISO/IEC 20000-1 به‌صورت قسمتی از تعریف ۳-۱(رخداد امنیت اطلاعات) استفاده شده است. رویداد ۲-۱۵ (نه رویداد امنیت اطلاعات) در موارد زیر به‌کار می‌رود: ۱. به تعریف مخاطره – ۳-۲۵ مراجعه شود که شامل یادآوری ۳ و ۴ با اشاره به رویداد است. ۲. تعریف تداوم خدمات ۳-۲۸ ۳. استاندارد ISO/IEC 20000-1 در بند ۶-۲- گزارش خدمات

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
			۴. استاندارد ISO/IEC 20000-1 در بند ۶-۳-۲ طرح‌های تداوم خدمات و در دسترس بودن به «رویداد» مراجعه شود: یک یا تعداد بیشتری رویداد می‌تواند قسمتی از رخداد امنیتی را شکل دهد.
رخداد امنیت اطلاعات	۲-۳۶ یک یا مجموعه‌ای رویدادهای ناشناخته یا غیرمنتظره‌ی امنیتی (۲-۳۶) که دارای احتمال زیادی از ترکیب کردن عملیات کسب‌وکار و تهدید کردن امنیت اطلاعات است (۲-۳۳)	۳-۱۲ یک یا مجموعه‌ای رویدادهای ناشناخته یا غیرمنتظره‌ی امنیتی (۲-۳۶) که دارای احتمال زیادی از ترکیب کردن عملیات کسب‌وکار و تهدید کردن امنیت اطلاعات است (استاندارد ISO/IEC 27000)	تعریف ۳-۱۲ در استاندارد ISO/IEC20000-1 شامل اصطلاح رخداد امنیت اطلاعات می‌شود. بند ۶-۶-۳ در استاندارد ISO/IEC20000-1شامل الزاماتی است: رخدادهای امنیت اطلاعات باید با استفاده از روش پیاده‌سازیی مدیریت رخداد مدیریت شود با اولویت مناسب با مخاطرات امنیت اطلاعات برای «چیزهایی که دارای مغایرت با خدمات هستند» و سبب مساله می‌شوند، ارائه نشده است، این چیزها علت یک یا تعداد بیشتری رخداد می‌شوند وقتی علت ریشه‌ای در زمان خلق مساله شناخته نشده است و فرایند مدیریت مساله برای بررسی‌های بیشتر دارای مسئولیت است. این‌ها توسط فرایند مدیریت مساله مدیریت شده‌اند و نه توسط مدیریت رخداد و فرایند درخواست خدمات. رخدادهای عمده (امنیت اطلاعاتی) توسط رخدادها و فرایند درخواست خدمات ارجاع داده شده، مدیریت شده‌اند. تغییرات در روشی که اصطلاحات استفاده شده‌اند در هر دو استاندارد پیچیده‌تر از رویداد یا رخداد امنیتی زیر مجموعه یا نوعی مشخص از رخدادها است. به بند ۶-۲-۵ این استاندارد مراجعه شود.
مدیریت رخداد امنیت اطلاعاتی	۲-۳۷ فرایندها (۲-۶۱) برای آشکارسازی، گزارش دادن، ارزیابی کردن و پاسخ دادن؛	تعریف نشده	رخداد رخداد امنیت اطلاعات خطای شناخته شده مساله

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
	مواجهه و یادگیری از رخدادهای امنیت اطلاعات (۲-۳۶)		مشاهده شود
یکپارچگی	۲-۴۰ خصوصیت دقت و کامل بودن	تعریف نشده	کلمه‌ی یکپارچگی در استاندارد ISO/IEC 20000-1 در معنای خود در انگلیسی عادی به‌کار رفته است: کیفیت یا حالت کامل بودن یا معیوب نبودن (به طور مثال به بند ۶-۶-۲ در استاندارد ISO/IEC 20000-1 مراجعه شود: «فراهم‌کننده خدمت باید واپایش‌های امنیت اطلاعات را به‌صورت فیزیکی، پیاده‌سازیی و فنی انجام دهد تا a) حفاظت از قابلیت اطمینان، یکپارچگی و دسترسی‌پذیری دارایی‌های اطلاعاتی» استاندارد ISO/IEC 20000-1 در بند ۹ شامل الزامات می‌شود: «باید روند پیاده‌سازیی مستندی برای ثبت کردن، واپایش کردن نسخه‌های CI ها وجود داشته باشد. درجه‌ی واپایش باید یکپارچگی خدمات را حفظ کند و الزامات خدمت و مخاطرات مورد متناظر با CI ها در نظر گیرد». «تغییرات CI ها باید قابل‌ردیابی و بازبینی باشد تا از یکپارچگی CIها و داده‌ها در CMDB اطمینان حاصل شود.» استاندارد ISO/IEC 20000-1 در بند ۹-۳ شامل الزاماتی می‌شود: «آزادسازی باید به محیط زنده گسترش یابد به گونه‌ای که یکپارچگی سخت‌افزاری، نرم‌افزاری و مولفه ی خدمات در مدت گسترش نگهداشته شود.»
طرف ذی‌نفع	۲-۴۱- شخص یا سازمانی (۲-۵۷) که می‌تواند توسط تصمیم یا اقدامی تاثیر بگذارد یا تاثیر بپذیرد	۳-۱۳- شخص یا گروهی دارای علایق مشخص در روش پیاده‌سازیی یا موفقیت اقدام یا اقدامات فراهم‌ساز	به «فراهم‌ساز خدمت» مراجعه شود. استاندارد ISO/IEC 27000 بر اصل قسمت ذی‌نفع تاکید دارد. استاندارد ISO/IEC 20000-1 بر علایق آن‌ها به عنوان معیار کلیدی تاکید دارد.

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		خدمت. مثال مشتری، مالک، مدیر، افراد در سازمان فراهم‌ساز خدمت، تامین کنندگان، بانکداران، اتحادیه یا طرف‌ها. یادآوری ۱- گروهی می‌تواند سازمان یا بیش از یک سازمان را تشکیل دهد، یادآوری ۲- از ISO 9000:2005 اقتباس شده است.	
گروه داخلی	تعریف نشده	۳-۱۴- قسمتی از سازمان فراهم-ساز خدمت که به پیمات مستند شده با فراهم‌کننده خدمت برای کمک به طراحی، انتقال، تحویل و بهبود خدمات است. **یادآوری**- گروه داخلی خارج از دامنه کاربرد SMS فراهم‌ساز خدمت است.	به «فراهم‌ساز خدمت» مراجعه شود.
خطای معلوم	تعریف نشده	۳-۱۵- مساله که دارای ریشه‌ی شناسایی یا روشی برای کاهش یا حذف اثر آن بر خدمات توسط کار پیرامون آن است.	به «رخداد» یا «مساله» مراجعه شود.
مدیریت سامانه	۲-۴۶- مجموعه عنصرهای وابسته به هم یا دارای فعل و انفعال داخلی برای خط‌مشی‌های ایجاد شده (۲-۶۰) و اهداف (۲-۵۶) و فرایندها (۲-۶۱) برای کسب اهداف **یادآوری ۱**- سامانه مدیریت می‌تواند یک یا چند قاعده را نشانی دهد. **یادآوری ۲**- عنصرهای سامانه	سامانه مدیریت در یادآوری ۱ تعریف سامانهٔ مدیریت خدمت تعریف شده است: **یادآوری ۱**- سامانه مدیریت مجموعه‌ای عنصرهای وابسته به هم یا دارای فعل و انفعال داخلی برای خط‌مشی‌های ایجاد شده و اهداف و فرایندها برای کسب اهداف	به‌صورت وسیع در هر دو استاندارد به یک معنا است.

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
	شامل ساختار سازمان، نقش‌ها و مسئولیت‌ها، طرح‌ریزی، عملیات و... است. **یادآوری ۳**- دامنه کاربرد سامانه مدیریت ممکن است شامل کل یک سازمان، قسمت‌های مشخص و شناسایی شده‌ی سازمان یا یک یا تعداد بیشتری کارکرد در گروهی از سازمان‌ها باشد.		
سلب انکار	۲-۵۴- توانایی اثبات وقوع رویداد یا اقدام ادعا شده و هستارهای منشا آن است.	تعریف نشده یا استفاده نشده	فاقد معادل مستقیم
سازمان	۲-۵۷- فرد یا گروهی از افراد که وظایف خود را با مسئولیت‌ها، اختیارات و روابط بر عهده دارند تا به اهدافشان (۲-۵۶) دست یابند. یادآوری ۱- مفهوم سازمان شامل شرکت، موسسه‌ی حقوقی، واحد اقتصادی، تجارتخانه، خیریه، موسسه یا قسمت یا ترکیبی از آن‌ها است خواه ثبت شده باشد خواه نشده باشد، خواه عمومی باشد خواه خصوصی	۳-۱۷- گروهی از افراد و تجهیزات با آرایش مسئولیت‌ها، صلاحیت‌ها و روابط مثال: شرکت، موسسه‌ی حقوقی، واحد اقتصادی، موسسه، خیریه، تجارتخانه یا قسمت یا ترکیبی از آن‌ها یادآوری ۱- آرایش عموما مرتب است. یادآوری ۲- سازمان می‌تواند خصوصی یا عمومی باشد (ISO 9000:2015)	استاندارد ISO/IEC 20000-1 از اصطلاح «فراهم کننده خدمت» و «سازمان» برای ساختارهای متفاوت استفاده می‌کند، بنابراین به‌صورت چشم‌گیری در هر توضیحی برای سامانه یکپارچه مدیریت متفاوت است. در استاندارد ISO/IEC 27000، سازمان ممکن است قسمت از ساختار بزرگ‌تر باشد مانند شرکت یا خیره به «فراهم‌کننده خدمت» مراجعه شود.
خط‌مشی	۲-۶- خواسته‌ها و جهت‌گیری سازمان (۲-۵۷) که توسط مدیریت ارشد (۲-۴۸) به صورت رسمی بیان شده است.	تعریف شده	کلمه‌ی خطشی در استاندارد ISO/IEC 20000-1 با همان معنای خود در انگلیسی متداول به‌کار رفته است: طرحی از اقدامات معمولا بر مبنای اصول قطعی، توسط بدنه یا فرد تصمیم‌گیری شده، اصل یا مجموعه اصول برای تصمیمات پایه، مسیری که از آن باید پیروی شود. خط‌مشی‌ها در استاندارد ISO/IEC 20000-1 برای جهت‌گیری مدیریت استفاده شده‌اند. توسط استاندارد ISO/IEC 20000-1 مواردی از جمله

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
			خط‌مشی مدیریت خدمت مورد نیاز است. استفاده از آن به‌صورت کلی در هر دو استاندارد یکسان است.
عمل ممانعت کننده	تعریف نشده	۳-۱۸- اقدامی برای جلوگیری یا حذف نمودن دلایل یا کاهش همسایگی پیشامدهای عدم تطابق یا دیگر موقعیت‌های نامطلوب **یادآوری**- از ISO 9000:2005 اقتباس شده است.	تعریف استاندارد ISO/IEC 20000-1 از تعریف دیکشنری دو اصطلاح بسط یافته است (همان‌طور که توسط پیش‌فرض در دنباله‌های 2700X استفاده شده است) تا شامل عمل ممانعت اوری شود که مانع علت نمی‌شود اما به شیوه‌هایی پیرامون آن کار می‌کند تا از تاثیر آن جلوگیری کند. در مدیریت خدمت همیشه عمل جلوگیری کننده ممکن یا مطلوب نیست و در واقع، می‌توانند بهتر و با ارزش‌تر باشد که از وقوع پیشامد اجتناب کرد. لذا برای استاندارد ISO/IEC 20000-1، تعریف ISO 9000 برای ایجاد این امکان اقتباس شده است. این‌ها برای اقدامات تصحیح کننده در تعریف ۳-۶ در استاندارد ISO/IEC 20000-1 و تعریف ۲-۱۹ در استاندارد ISO/IEC 27000 پیوند یافته‌اند.
مساله	تعریف نشده	۳-۱۹ عامل ریشه‌ای یک یا تعداد بیشتری رخداد است. **یادآوری**- عامل ریشه‌ای معمولا در زمانی که ثبت مساله خلق شده است، شناخته نشده و فرایند مدیریت مساله برای بررسی بیشتر منطقی است.	به «رخداد» یا «خطای شناخته شده» مراجعه شود.
روش اجرایی	تعریف نشده	۳-۲۰ روشی مشخص برای پیاده‌سازی فعالیت یا فرایند (استاندارد ISO/IEC 9000:2005) **یادآوری**- روش پیاده‌سازی می‌تواند مستند شود یا نشود.	تعریف استفاده شده توسط استاندارد ISO/IEC 20000-1 بر مبنای تعریف ISO 9000 است. به‌صورت گسترده شبیه به هم هستند. تنها یادآوری ها متفاوت‌اند؛ یعنی روش پیاده‌سازی می‌توانند مستندسازی نشوند؛ اما ارجاع‌های استاندارد ISO/IEC 20000-1 به روش پیاده‌سازی همگی به «روش پیاده‌سازی مستندسازی شده» هستند. آن روش‌های

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
			پیاده‌سازیی که قسمتی از طرح هستند به‌صورت قسمتی از طرح مستندسازی شده‌اند.
فرایند	۲-۶۱- مجموعه از فعالیت‌های مرتبط و متعامل که ورودی‌ها را به خروجی‌ها تبدیل می‌کنند. (ISO 9000:2005)	۳-۲۱- مجموعه از فعالیت‌های وابسته به هم و دارای فعل‌وانفعالات داخل که ورودی‌ها را به خروجی‌ها منتقل می‌کنند. (ISO 9000:2005)	هر دو بر مبنای ISO 9000:2005
ثبت	در متن اصلی استاندارد ISO/IEC 27001 تعریف نشده یا استفاده نشده	۳-۲۲- سند بیان‌کننده‌ی نتایج اکتساب شده یا ارائه دهنده ی مدرک فعالیت‌های عمل شده است	تعریف استاندارد ISO/IEC 20000-1 بر مبنای ISO 9000:2005 است. استاندارد ISO/IEC 27001 از عبارت «اطلاعات مستندسازی شده» به جای اصطلاح «ثبت» استفاده می‌کند.
واگذار کردن	تعریف یا استفاده نشده است	۳-۲۳- مجموعه‌ای از یک یا تعداد بیشتری CI های جدید یا تغییر کرده که برای محیط زنده به‌صورت نتایج یک یا تعداد بیشتری تغییرات به‌کار گرفته شده‌اند.	استاندارد ISO/IEC 27001 در پیوست الف به «مدیریت تغییرات» به‌صورت واپایش در A-10-1-2 اشاره دارد. بسیاری از واپایش‌ها در استاندارد ISO/IEC 27001 اشاره به مدیریت یا واپایش تغییرات است. برای مثال: A-8-3- و A-10-2-3 و A-12-5-1
اطمینان‌پذیری	۲-۶۲ خصوصیت ثبات و پایداری در رفتار و نتایج مورد نظر است.	با اشاره به 3-11 امنیت اطلاعات: **یادآوری ۱-** دیگر خصوصیات مانند اصالت‌سنجی، جوابگویی و قابلیت اعتماد نیز در گیر می‌شوند.	کلمه‌ی «قابلیت اعتماد» در استاندارد ISO/IEC 20000-1 با همان معنای متداول خود در انگلیسی به‌کار رفته است: قابلیت اعتماد استاندارد ISO/IEC 20000-1 بند 9-1 را مشاهده کنید: CMDB باید مدیریت شود تا از دقت و قابلیت اعتماد آن اطمینان کسب شود، از جمله واپایش به روز دسترسی
مخاطره	۲-۶۸ اثر عدم قطعیت بر اهداف است. **یادآوری ۱-** اثر، انحراف از انتظار است که می‌تواند مثبت یا منفی	۳-۲۵- اثر عدم قطعیت اهداف **یادآوری ۱-** اثر انحرافی از مثبت/منفی مورد انتظار است. **یادآوری ۲-** اهداف می‌تواند	استفاده‌ی روشن محدودی از «مخاطره» در استاندارد ISO/IEC 20000 وجود دارد، اگرچه بسیاری از جنبه‌های فعال مدیریت خدمت به کمک مخاطره‌های کاهش‌دهنده می‌آیند.

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
	باشد. **یادآوری ۲**- عدم قطعیت حالتی از فقدان اطلاعات مربوط به درک یا اطلاعات یک رویداد_۲-۴۵)، عواقب آن (۲-۱۴) یا احتمال(۲-۴۵) است. **یادآوری ۳**- مخاطره اغلب توسط مرجع برای رویدادها (۲-۲۵) و عواقب آن (۲-۱۴) یا ترکیب آن‌ها مشخص شده‌اند. **یادآوری ۴**- مخاطره اغلب در اصطلاح ترکیب عواقب رویداد (شامل تغییرات در پیشامدها)(۲-۱۴) و احتمال متناظر رخداد (۲-۴۵) بیان شده است. **یادآوری ۵**- دربارهٔ سامانه‌های امنیت اطلاعات، مخاطره‌های امنیت اطلاعات می‌تواند به‌صورت اثر عدم قطعیت در اهداف بیان شده باشد. **یادآوری ۶**- مخاطره‌ی امنیت اطلاعات متناظر با هدفی است که تهدیدها (۲-۸۳) از آسیب‌پذیری‌های (۲-۸۹) دارایی اطلاعاتی یا گروهی از دارایی‌های اطلاعاتی بهره‌جویی می‌کنند و سبب آسیب به سازمان می‌شوند.	دارای جنبه‌های زیادی باشد (مانند اهداف اقتصادی، سلامت، امنیت و محیط زیستی) و می‌تواند در سطوح مختلفی اعمال شود (مانند راهبردی، سازمانی، پروژه‌ای، محصول و فرایند) **یادآوری ۳**- مخاطره اغلب توسط مرجع برای رویدادها (2-17) و عواقب آن (2-18) یا ترکیب آن‌ها مشخص شده‌اند. **یادآوری ۴**- مخاطره اغلب در اصطلاح ترکیب عواقب رویداد شامل تغییرات در پیشامدها و احتمال متناظر رخداد (2-19) بیان شده است. **یادآوری ۵**- عدم قطعیت حالتی از فقدان اطلاعات مربوط به درک یا اطلاعات یک رویداد، عواقب آن یا احتمال است. (راهنمای ISO، ۷۳:۲۰۰۹ ، تعریف ۱-۱)	استاندارد ISO/IEC 27000 در تفسیر مخصوص مخاطره‌ی امنیت اطلاعات، معرفی کننده‌ی مفهوم آسیب‌پذیری و تهدید هستند. همچنین بیان شده که مخاطرات امنیت اطلاعات می‌تواند بر حسب اصطلاحات توصیف شود که دربارهٔ چگونگی اثرگذاری آن‌ها بر اهداف امنیت اطلاعات به جای اهداف کلی سازمان است. لازم به ذکر است که مفهوم «مخاطره» در استاندارد ISO/IEC 27001 تحت بازبینی به همان صورتی است که در استاندارد ISO/IEC 20000-1 بر مبنای ISO 31000 تعریف شده است. به «آسیب‌پذیری» مراجعه شود.
پذیرش مخاطره	۲-۶۹- تصمیم آگاهانه برای به عهده گرفتن مخاطره (۲-۶۸) خاص است. (منبع: راهنمای ISO 73:2009) **یادآوری ۱**- پذیرش مخاطره می‌تواند بدون حذف مخاطره (۲-۷۹) یا در زمان فرایند حذف مخاطره باشد. **یادآوری ۲**- مخاطرات پذیرفته شده تحت پایش (۲-۵۲) و بازبینی (۲-۶۵) هستند.	تعریف نشده	عبارت «پذیرش مخاطره» در استاندارد ISO/IEC 20000-1تعریف یا استفاده نشده است. هرچند در استاندارد ISO/IEC 20000-1 الزاماتی برای تعریف کردن معیار پذیرش مخاطره در طرح مدیریت خدمت (بند ۴-۵-۲) و در فرایند مدیریت امنیت اطلاعات (بند ۶-۶-۱) وجود دارد. مفاهیم مشابه در بند ۵-۴ در الزامات برای استفاده از معیار پذیرش هستند.
تحلیل مخاطره	۲-۷ فرایند درک ماهیت مخاطره	تعریف نشده	به «ارزیابی مخاطره» مراجعه شود. توصیه می‌شود دقت زیاد به‌کار برد، ارزیابی مخاطره

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
	(۲۰۶۸) و تعیین سطح مخاطره (۲-۴۴) است. **یادآوری ۱-** تحلیل مخاطره اساسی برای ارزیابی مخاطره (۲-۷-۴) و تصمیم‌گیری دربارهٔ حذف مخاطره ارائه می‌دهد.		از نظر تعریف مشابه «پذیرش مخاطره» نیست. برای اطلاعات بیشتر به استاندارد ISO/IEC 27005 مراجعه شود.
ارزیابی مخاطره	۲-۷۱ فرایند (۲-۶۱) کلان شناسایی مخاطره (۲-۷۵)، تحلیل مخاطره (۲-۷۰) و ارزیابی مخاطره (۲-۷۴).	تعریف نشده	مراجع در استاندارد ISO/IEC 20000-1 برای ارزیابی مخاطره متناسب با خدمات هستند. برای مثال: بند ۴-۵-۳-: (پیاده‌سازی و عمل کردن SMS) شامل d) شناسایی ارزیابی و مدیریت مخاطرات خدمات بند ۵-۲ (طرح‌ریزی خدمات جدید یا تغییر کرده) شامل f) شناسایی، ارزیابی و مدیریت مخاطرات. بندی ۶-۶-۱d :) کسب اطمینان از اینکه ارزیابی مخاطره‌ی امنیتی در محدوده‌ای طرح‌ریزی شده انجام شده‌اند.
ارتباطات مخاطره	۲-۷۲ ارتباطات مخاطره و مشاوره‌ی پیوسته و فرایندهای تکراری که سازمانی به منظور ارائه نمودن، به اشتراک‌گذاری یا کسب اطلاعات و به منظور استفاده در محاوره ی بین سهامداران (۲-۸۲) با توجه با مدیریت خدمت (۲-۶۸) انجام می‌دهد. **یادآوری ۱-** اطلاعات می‌تواند مربوط به وجود، طبیعت، قالب، احتمال، اهمیت، ارزیابی، مقبولیت و حذف مخاطره باشد. **یادآوری ۲-** مشاهده فرایندی ۲ راهی از ارتباطات بین سازمان و سهامداران آن در موضوعی پیش از تصمیم‌گیری یا تعیین جهت‌گیری نسبت به موضوع است. مشاوره: فرایندی است که بر تصمیمات به	تعریف نشده	در استاندارد ISO/IEC 20000-1 در هر روش مربوط به مخاطره استفاده نشده است.

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
	واسطه‌ی تاثیر به جای توان، اثر گذار است و ورودی تصمیم‌گیری و نه مفصل تصمیم‌گیری است.		
معیار مخاطره	۲-۷۳ اصطلاحات مرجع در برابر اهمیت مخاطره (۲-۶۸) ارزیابی شده است. **یادآوری ۱**- معیار مخاطره بر مبنای اهداف سازمان و محتوای داخلی و خارجی است. **یادآوری ۲**- معیار مخاطره از استانداردها، قوانین، خط‌مشی‌ها و دیگر الزامات استنتاج شده است.	تعریف نشده	در استاندارد ISO/IEC 20000-1 مشابه با استاندارد ISO/IEC 27001 استفاده شده است. به طور مثال بند ۴-۵-۲- در استاندارد ISO/IEC 20000-1 "طرح مدیریت خدمت باید شامل مرجعی برای ... j) رویکردی برای مدیریت مخاطرات و معیار مقبولیت مخاطره باید در نظر گرفته شود. مفهوم برای هر دو استاندارد مشابه است، اما در استاندارد ISO/IEC 27001 دارای اهمیت بیشتری نسبت به استاندارد ISO/IEC 20000-1 است.
ارزیابی مخاطره	۲-۷-۴ فرایند (۲-۶۱) مقایسه کننده نتایج تحلیل مخاطره (۲-۷۰) با معیار مخاطره _۲-۷۳) برای تعیین نمودن اینکه آیا مخاطره (۲-۶۸) و بزرگی آن قابل قبول است. **یادآوری**- ارزیابی مخاطره در تصمیم‌گیری دربارهٔ حذف مخاطره تاثیر دارد (۲-۷۹)	تعریف نشده	به «ارزیابی مخاطره» مراجعه شود.
شناسایی مخاطره	۲-۷۵ فرایند یافته‌ها و شناسایی و توصیف مخاطرات (۲-۶۸) **یادآوری ۱**- شناسایی مخاطره، شناسایی منابع مخاطره، رویدادها و دلایل و عواقب آن‌ها است. **یادآوری ۲**- شناسایی مخاطره می‌تواند شامل تاریخچه‌ی داده‌ها، تحلیل تئوری، گزینه‌های ویژه و اطلاع داده شده و نیازهای سهامداران باشد.	تعریف نشده	به «ارزیابی مخاطره» مراجعه شود.
مدیریت مخاطره	۲-۷۶- فعالیت‌های هماهنگ شده برای جهت‌گیری و واپایش	تعریف نشده	به‌صورت گسترده در هر دو استاندارد به یک معنا است.

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
	سازمان (۲-۵۷) با توجه به مخاطره		
مالک مخاطره	۲-۷۸ شخص یا هستار که مسئولیت پاسخ‌گویی و اختیار مدیریت مخاطره را دارد (۲-۶۸)	تعریف نشده	به‌صورت گسترده در هر دو استاندارد به یک معنا است
حذف مخاطره	۲-۷۹ فرایند (۲-۶۱) برای اصلاح مخاطره (۲-۶۸) **یادآوری ۱**- حذف مخاطره می‌تواند موارد زیر را درگیر کند: - اجتناب کردن از مخاطره توسط تصمیم‌گیری آغاز نکردن یا ادامه نداد فعالیتی که مخاطره ایجاد می‌کند. - افزایش دادن مخاطره برای بررسی کردن شانس - حذف منبع مخاطره - تغییر احتمال کلی - تغییر عواقب - اشتراک‌گذاری مخاطره با طرف دیگر (شامل پیمانکاران و نامزد مخاطره و - نگاه داشتن مخاطره توسط انتخاب آگهی دهنده **یادآوری ۲**- حذف مخاطره‌ای که با عواقب منفی روبرو می‌شود گاها به‌صورت «کاهش مخاطره»، «حذف مخاطره» «جلوگیری از مخاطره» و «کاهش مخاطره» است. **یادآوری ۳**- حذف مخاطره می‌تواند مخاطرات جدید ایجاد کند یا مخاطرات موجود را اصلاح کند.	تعریف نشده	اصطلاح «حذف مخاطره» در استاندارد ISO/IEC 20000-1 استفاده نشده؛ این اصطلاح توسط اصطلاح «مدیریت مخاطره» پوشش داده شده، (به مثال‌هایی از «ارزیابی مخاطره» مراجعه شود.)
خدمات	تعریف نشده	۳-۲۶- ابزاری برای تحویل ارزش	فاقد معادل مستقیم

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		به مشتری توسط تسهیل کردن نتایجی که مشتری خواستار رسیدن به آن است. یادآوری ۱- خدمات به طور عموم ناملموس هستند.	
مولفه ی خدمات	تعریف نشده	۳-۲۷ واحدی منفرد از خدمات که زمانی که با دیگر واحدها ترکیب می‌شود خدمتی کامل را تحویل می‌دهد. مثال‌ها سخت‌افزار، نرم‌افزار، ابزارها، برنامه‌های کاربردی؛ مستندات، اطلاعات؛ فرایندها یا خدمات پشتیبانی **یادآوری**- مولفه‌ی خدماتی می‌تواند شامل یک یا تعداد بیشتر Ci باشد.	فاقد معادل مستقیم
تداوم خدمات	تعریف نشده	۳-۲۸- ظرفیت مدیریت کردن مخاطره و رویدادهایی که می‌تواند دارای تاثیر جدی بر خدمات به منظور تحویل پیوسته‌ی خدمات در سطوح مقبول باشد.	«آسیب‌پذیری» و «مخاطره» و «تداوم کسب‌وکار» مشاهده شود. تداوم خدمات به‌صورت عادی به‌صورت زیر مجموعه‌ای از تداوم کسب‌وکار در نظر گرفته می‌شود.
مقبولیت سطح خدمات	تعریف نشده	۳-۲۹- پذیریش مستند بین فراهم‌کننده خدمت و مشتری که خدمات و اهداف آن را شناسایی می‌کند. **یادآوری ۱**- مقبولیت سطح خدمات می‌تواند بین فراهم‌ساز خدمت و تامین کننده، گروه داخلی یا مشتری پایه برقرار	این اصطلاح در استاندارد ISO/IEC 27001 استفاده نشده است. هر چند، این مفهوم در رابطه با اهداف واپایشی A-1-2 در نظر گرفته شده است، آن هم زمانی که جنبه‌های خدمات تحویل یافته و نگهداری شده توسط طرف سوم در نظر گرفته شده‌اند به طور مثال واپایش A-10-2-1 (سطوح تداوم خدمات پذیرفته شده)

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		شود. **یادآوری ۲**- مقبولیت سطح خدمت می‌تواند در قرارداد یا انواع دیگر مقبولیت‌های مستند قرار گیرد.	
مدیریت خدمت	تعریف نشده	۳-۳۰ مجموعه‌ای توانایی‌ها و فرایندها برای جهت‌گیری و واپایش فعالیت‌های فراهم-کننده خدمت و منابع برای طراحی، انتقال، تحویل و بهبود خدمات برای برآورده نمودن الزامات خدمت	اهداف واپایشی A-10-2 در استاندارد ISO/IEC 27001 مربوط به این اصطلاح هستند.
سامانهٔ مدیریت خدمت SMS	تعریف نشده	۳-۳۱ سامانه مدیریت برای جهت‌گیری و واپایش فعالیت‌های مدیریت خدمت فراهم‌کننده خدمت **یادآوری ۱**- سامانه مدیریت مجموعه‌ای عنصرهای دارای اشتراک داخلی و دارای فعال وانفعال داخلی است که برای پایه‌گذاری خط‌مشی‌ها و اهداف به منظور نیل به اهداف است. **یادآوری ۲**- SMS شامل تمامی خط‌مشی‌های مدیریت خدمت، اهداف، طرح‌ها، فرایندها، مستندات و منابع مورد نیاز برای طراحی، انتقال تحویل و بهبود خدمات و برای کامل نمودن الزامات در این قسمت از استاندارد ISO/IEC 20000-1 است. **یادآوری ۳**- با پذیرش تعریف «سامانهٔ مدیریت کیفیت» در استاندارد ISO/IEC 9000:2005	به اصطلاح «سامانهٔ مدیریت خدمت ISMS» در استاندارد ISO/27001 برای توصیف نمودن سازمان در دامنه کاربرد مدیریت امنیت اطلاعات است «سازمان» مراجعه شود.
فراهم‌کننده خدمت	تعریف نشده	۳-۳۲- سازمان یا قسمتی از سازمان که خدماتی را برای	«فراهم‌ساز خدمت» در تعریف ۳۰۳۲ در استاندارد ISO/IEC 20000-1 سازمانی است که برای برآورده نمودن الزامات

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		مشتری مدیریت و ارائه می‌کند. **یادآوری ۱**- مشتری می‌تواند برای سازمان فراهم‌کننده خدمت داخلی یا خارجی باشد.	استاندارد ISO/IEC 20000-1 ارزیابی می‌شود. این اصطلاح استفاده شده است زیرا بین فراهم‌ساز خدمت و دیگر گروه‌ها (که مشتری و طرف‌های دیگر (تامین کننده، گروه‌های داخلی، مشتری هستند)، سازمان‌های خارجی، طرف‌های ذی‌نفع یا فراهم‌کننده خدمت با ابزاری که عملیات SMS را پشتیبانی می‌کند، فاصله‌ای ایجاد می‌کند. فراهم‌ساز خدمت می‌تواند قسمتی از سازمان بزرگ‌تر یا کل یک سازمان باشد.
درخواست خدمات	تعریف نشده	۳-۳۳ درخواست دادن اطلاعات، توصیه، دسترسی به خدمات یا تغییرات از پیش تصدیق شده	فاقد معادل مستقیم
الزامات خدمت	تعریف نشده	۳-۳۴- نیاز مشتری و کاربران خدمات، شامل الزامات سطح خدمات و نیازهای فراهم‌کننده خدمت	الزامات خدمت در تعریف ۳-۳-۴ در استاندارد ISO/IEC 20000-1 ارائه شده است. در استاندارد ISO/IEC 27001 «الزامات» با معنای عادی خود در انگلیسی استفاده شده است: نیاز داشتن، چیزی مورد درخواست، ضروری، سفارش داده شده در استاندارد ISO/IEC 27001 به‌صورت «الزامات خدمت» استفاده نشده‌اند، اگرچه استفاده‌های مختلفی از «الزامات امنیتی» قانونی یا دیگر موارد وجود دارد.
تامین کننده	تعریف نشده	۳-۳۵- سازمان یا قسمتی از سازمان که برای سازمان فراهم‌ساز خدمت خارجی محسوب می‌شود و با قرارداد با فراهم‌ساز خدمت طراحی، انتقال، تحویل و بهبود خدمت یا فرایندهایی	استاندارد ISO/IEC 20000-1شامل منابع و الزاماتی برای مدیریت کردن موارد زیر می‌شود: الف- تامین کننده ب- تامین کنندگان اصلی (که تامین کنندگان جز را مدیریت می‌کنند.) پ- گروه‌های داخلی (فراهم‌کننده خدمت) ت- مشتری (هنگام فعالیت به‌صورت تامین

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		را بر عهده می‌گیرد. **یادآوری**- تامین کنندگان شامل تامین کنندگان اختصاص یافته می‌شود اما پیمان‌کارانِ آن تامین کنندگان را شامل نمی‌شود.	کننده) تمامی کمک‌ها برای خدمات توسط فراهم-ساز خدمت مدیریت می‌شوند. مدیریت خدمت تامین کنندگان؛ تامین کنندگان اصلی (به همراه تامین کنندگان اصلی، تامین کنندگان فرعی نیز هستند) را پوشش می‌دهد. در هنگام فعالیت به عنوان تامین کننده، مدیریت سطح خدمات مدیریت گروه‌های داخلی و مشتریان را پوشش می‌دهد. استاندارد ISO/IEC 27001 فقط یک‌بار از اصطلاح «تامین کننده» استفاده کرده است.
تهدید	۲-۸۳ عامل بالقوهٔ رخدادی ناخواسته که ممکن است باعث آسیب-رسانی به سامانه یا سازمان شود.	تعریف نشده	در استاندارد ISO/IEC 20000-1 اصطلاح «حذف کردن» یک‌مرتبه استفاده شده؛ در تعریف ۳-۱۲: «رخداد امنیت اطلاعات: یک یا مجموعه‌ای رویدادهای ناخواسته و غیرقابل انتظار امنیت اطلاعات که دارای احتمال زیادی از ترکیب کردن عملیات کسب‌وکار و حذف کردن امنیت اطلاعات است»
مدیریت ارشد	۲-۸۴ فرد یا گروهی از اشخاص که سازمان را در بالاترین سطح هدایت و واپایش می‌کند. **یادآوری ۱**- مدیریت ارشد دارای قدرت محول کردن صلاحیت و فراهم‌سازی منابع درون سازمان است. **یادآوری ۲**- اگر دامنه کاربرد سامانهٔ مدیریت (۲-۴۶) تنها قسمتی از سازمان را پوشش دهد (۲-۵۷) آنگاه مدیریت ارشد به کسانی اشاره می‌کند که ان قسمت از سازمان را هدایت و واپایش می‌کنند.	۳-۳۶ شخص یا گروهی از اشخاص که فراهم‌ساز خدمت را هدایت و واپایش می‌کند آن هم در بالاترین سطح **یادآوری**- از استاندارد ISO 9000:2005 گرفته شده است.	در استاندارد ISO/IEC 27000«مدیریت ارشد» می‌تواند به شخص یا گروهی از افراد ارجاع شود که در بالاترین سطح کل سازمان نیستند اما به جای آن در بالاترین قسمتی هستند که در دامنه کاربرد برای ISMS است. سازمان همچنین می‌تواند دارای نقشی به عنوان فراهم‌ساز خدمت باشد. «سازمان» مشاهده شود.
انتقال	تعریف نشده	۳-۳۷ فعالیت‌هایی که در حرکت	بین انتقال (بند ۵ در استاندارد ISO/IEC 20000-1) و روشی که در آن بعضی از

اصطلاح	استاندارد ISO/IEC 27000	استاندارد ISO/IEC 20000-1	توضیحات استفاده از اصطلاح مورد نظر در هر دو استاندارد
		دادن خدمات جدید یا تغییریافته ای محیط رنده در گیرند	تغییرات مطابق با استاندارد ISO/IEC 27001 واپایش شده‌اند، تغییراتی وجود دارد. فرایندهای واپایشی در بند ۵ و ۹ در استاندارد ISO/IEC 20000-1 توصیف شده‌اند و به‌صورت نزدیک به این مفهوم پیوند داده شده‌اند. استاندارد ISO/IEC 27001 مدیریت تغییرات را در بندهای زیر ساماندهی می‌کند: A-10-1-2: مدیریت تغییرات روند عملیات و مسئولیت‌ها A-10-2-3 مدیریت تغییرات برای خدمات طرف سوم
آسیب‌پذیری	۲-۸۹ ضعف دارایی یا واپایش (۲-۱۶) که می‌تواند توسط یک یا تعداد بیشتری تهدید بهره‌جویی شود.	استفاده یا تعریف نشده	فاقد معادل مستقیم

کتاب‌نامه

[1] ISO 9000, Quality management systems — Fundamentals and vocabulary

[2] ISO/IEC/TS 15504-8, Information technology — Process assessment — Part 8: An exemplar process assessment model for IT service management

[3] ISO 19011, Guidelines for auditing management systems

[4] ISO/IEC 20000-2, Information technology — Service management — Part 2: Guidance on the application of service management systems

[5] ISO/IEC 20000-3, Information technology — Service management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1

[6] ISO/IEC/TR 20000-4, Information technology — Service management — Part 4: Process reference model

[7] ISO/IEC/TR 20000-5, Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1

[8] ISO/IEC/TR 20000-9, Information technology — Service management — Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services

[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 — Code of practice for information security controls

[11] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance

[12] ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement

[13] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[14] ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[15] ISO/IEC 27007, Information technology — Security techniques — 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 for inter-sector and inter-organizational communications

[18] ISO/IEC 27014, Information technology — Security techniques — Governance of information security

[19] ISO 31000, Risk management — Principles and guidelines

[20] ISO Guide 73:2009, Risk management — Vocabulary