INSO-ISO-IEC
27000
1st. Edition
Identical with
ISO/IEC
27000:2009
Jan.2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استانداردایران ایزو-آی‌ای سی
۲۷۰۰۰
چاپ اول
دی ۱۳۹۱

فناوری اطلاعات- فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان

Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

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

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

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

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

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

1- International Organization for Standardization

2 - International Electrotechnical Commission

3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی-سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان»

رئیس	**سمت و/یا نمایندگی**
داننده، آزاده (لیسانس مهندسی کامپیوتر)	رئیس نظام امور صنفی و رایانه
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا : (اسامی به ترتیب حروف الفبا)	
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسئول سازمان فناوری اطلاعات
بختیاری، شیرین (لیسانس مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
بداغی، امیرحسین (فوق لیسانس مهندسی برق)	کارشناس سازمان فناوری اطلاعات
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
خراسانی راد، ایمان (لیسانس مهندسی مکانیک)	مدیر عامل شرکت پایه‌ریزان راه کارهای فراگیر
رحیمی، مرتضی (فوق لیسانس مخابرات رمز)	کارشناس سازمان فناوری اطلاعات
رستمی، حبیب (فوق لیسانس ریاضی کاربردی)	مدیر گروه پژوهشی فناوری اطلاعات، جهاد دانشگاه صنعتی شریف

رشتی، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیرعامل شرکت توسعه ارتباطات بهینه برنا
سجادیه، سید علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
سعیدی، عذرا (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
سلطانی حقیقت، الهه (لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
شادمان، امید (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت هیرساویژن
شیرازی، مریم (لیسانس مهندسی فناوری اطلاعات)	کارشناس پژوهشگاه سازمان ملی استاندارد
صوفی زاده، جلیل (دکترای مهندسی مخابرات)	استاد دانشگاه و مشاور ارشد سازمان‌ها
طی نیا، رضا (فوق لیسانس فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
فخر عطار، رضا (فوق لیسانس مهندسی فناوری اطلاعات)	مشاور سازمان فناوری اطلاعات
فرمان آرا، شایسته (لیسانس کامپیوتر)	نماینده دفتر تدوین سازمان ملی استاندارد
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
فولادیان، مجید	مشاور سازمان فناوری اطلاعات

(فوق لیسانس مهندسی مخابرات)

فیاضی، مهدی (ششثقثلیسانس مهندسی الکترونیک)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات، لیسانس مهندسی الکترونیک)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قودجانی، ابوالفضل (فوق لیسانس آمار)	کارشناس سازمان فناوری اطلاعات
کبیری، پیمان (دکترای مهندسی کامپیوتر سخت افزار)	هیات علمی دانشگاه علم و صنعت
معروف، سینا (لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس سازمان فناوری اطلاعات
موجبی، محمود (فوق لیسانس مهندسی مخابرات رمز)	کارشناس سازمان فناوری اطلاعات
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رئیس اداره تدوین استانداردها و نظارت بر امنیت سرویس‌ها
میرمعینی، علیرضا (فوق لیسانس مهندسی صنایع)	مدیرعامل پژوهش های راهبردی امن رای
ناپلیان، کامران (فوق لیسانس فناوری اطلاعات)	کارشناس سازمان فناوری اطلاعات
ناصری، علی (دکترای مهندسی برق الکترونیک)	هیئت علمی دانشگاه امام حسین
یوسف زاده، بهاره (فوق لیسانس)	کارشناس سازمان ملی استاندارد

فهرست

آشنایی با سازمان ملی استاندارد ایران	ب
کمیسیون فنی تدوین استاندارد	ج
پیش‌گفتار	د
۰ مقدمه	ه
۰-۱ مرور کلی	و
۰-۲ استانداردهای خانواده ISMS	ز
۰-۳ هدف از این استاندارد ملی	ر
۱ هدف و دامنه کاربرد	۱
۲ اصطلاحات و تعاریف	۱
۳ سامانه‌های مدیریت امنیت اطلاعات	۱۰
۳-۱ مقدمه	۱۰
۳-۲ سامانه مدیریت امنیت اطلاعات (ISMS) چیست؟	۱۱
۳-۲-۱ مرور کلی و اصول	۱۱
۳-۲-۲ اطلاعات	۱۲
۳-۲-۳ امنیت اطلاعات	۱۲
۳-۲-۴ مدیریت	۱۳
۳-۲-۵ سامانه مدیریت	۱۳
۳-۳ رویکرد فرآیندی	۱۳
۳-۴ چرا ISMS مهم است؟	۱۴
۳-۵ برقراری، پایش، نگهداری و بهبود ISMS	۱۶
۳-۵-۱ مرور کلی	۱۶
۳-۵-۲ شناسایی الزامات امنیت اطلاعات	۱۶
۳-۵-۳ ارزشیابی مخاطرات امنیت اطلاعات	۱۶

۳-۵-۴ انتخاب و پیاده سازی کنترل‌های امنیت اطلاعات ۱۷
۳-۵-۵ پایش، نگهداری و بهبود اثربخشی ISMS ۱۷
۳-۶ عوامل مهم موفقیت ISMS ۱۷
۳-۷ مزایای استانداردهای خانواده ISMS ۱۸
۴ استانداردهای خانواده ISMS ۱۹
۴-۱ اطلاعات کلی ۱۹
۴-۲ استانداردهای توصیف کننده مرور کلی و واژگان ۲۰
۴-۲-۱ ISO/IEC 27000 (سند حاضر) ۲۰
۴-۳ استانداردهای مشخص کننده الزامات ۲۱
۴-۳-۱ ISO/IEC 27001 ۲۱
۴-۳-۲ ISO/IEC 27006 ۲۱
۴-۴ استانداردهای توصیف کننده راهنمای مرور کلی ۲۲
۴-۴-۱ ISO/IEC 27002 ۲۲
۴-۴-۲ ISO/IEC 27003 ۲۲
۴-۴-۳ ISO/IEC 27004 ۲۳
۴-۴-۴ ISO/IEC 27005 ۲۳
۴-۴-۵ ISO/IEC 27007 ۲۳
۴-۵ استانداردهای توصیف کننده راهنماهای بخش خاص ۲۴
۴-۵-۱ ISO/IEC 27011 ۲۴
۴-۵-۲ ISO 27799 ۲۴
پیوست الف ۲۵
پیوست ب ۲۶

پیش‌گفتار

استاندارد« فناوری اطلاعات- فنون امنیتی-سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان» که پیش نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۷/۱۶ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

منبع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 27000:2009, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

۰ مقدمه

۰-۱ مرور کلی

استانداردهای ملی سامانه‌های مدیریت، به منظور فراهم آوردن مدلی برای برپایی و بهره‌برداری[1] از سامانه مدیریت تهیه شده است. این مدل دربردارنده‌ی مشخصه‌هایی است که متخصصان این حوزه در مورد آن‌ها به عنوان فناوری بین‌المللی روز به اجماع رسیده‌اند. کمیته فرعی ISO/IEC JTC 1 SC 27[2]، شامل گروهی تخصصی است که به تدوین استانداردهای سامانه‌های مدیریت بین‌المللی امنیت اطلاعات می‌پردازد. این استانداردها به عنوان استانداردهای خانواده سامانه مدیریت امنیت اطلاعات (ISMS)[3] شناخته می‌شوند.

سازمان‌ها می‌توانند با استفاده از استانداردهای خانواده ISMS، چارچوبی را برای مدیریت امنیت دارایی‌های اطلاعاتی خود تدوین و پیاده‌سازی کنند و برای ارزشیابی[4] مستقل سامانه مدیریت امنیت اطلاعات خود، به منظور حفاظت از اطلاعاتی مانند اطلاعات مالی[5]، مالکیت معنوی[6] ، ریز اطلاعات کارکنان[7] یا اطلاعات سپرده شده به آن‌ها توسط مشتریان یا طرف سوم[8] آماده باشند.

۰-۲ استانداردهای خانواده ISMS

استانداردهای خانواده ISMS برای کمک به سازمان‌ها از هر نوع و اندازه، به منظور پیاده‌سازی و بهره‌برداری از ISMS در نظر گرفته شده است. استانداردهای خانواده ISMS شامل استانداردهای بین‌المللی زیر، با عنوان عمومی فناوری اطلاعات- فنون امنیتی است:

- استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان
- استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، سامانه‌های مدیریت امنیت اطلاعات- الزامات
- استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، آیین کار مدیریت امنیت اطلاعات
- ISO/IEC 27003، راهنمای پیاده‌سازی سامانه مدیریت امنیت اطلاعات

---

1 - Operating
2 - International Organization for Standardization/ International Electro-technical Commission Joint Technical Committee
3 - Information Security Management Systems
4 - Assessment
5 - Financial Information
6 - Intellectual Property
7 - Employee Details
8 - Third Parties

- ISO/IEC 27004[1]، مدیریت امنیت اطلاعات- سنجش
- ISO/IEC 27005:2008، مدیریت مخاطرات امنیت اطلاعات
- استاندارد ملی ایران شماره ۲۷۰۰۶: سال ۱۳۸۷، الزامات نهادهای ارائه‌دهنده خدمات ممیزی و صدور گواهی سامانه‌های مدیریت امنیت اطلاعات
- ISO/IEC 27007[2]، راهنمای ممیزی سامانه‌های مدیریت امنیت اطلاعات
- ISO/IEC 27011، راهنمای مدیریت امنیت اطلاعات برای سازمان‌های مخابراتی مبتنی بر ISO/IEC 27002

یادآوری- عنوان عمومی «فناوری اطلاعات- فنون امنیتی» نشان می‌دهد این استانداردها توسط کمیته فرعی ۲۷ با نام فنون امنیتی فناوری اطلاعات از کمیته فنی مشترک شماره یک[3] موسوم به فناوری اطلاعات، تدوین شده است.

استانداردهای بین‌المللی که تحت همین عنوان عمومی نیستند و در عین حال قسمتی از استانداردهای خانواده ISMS محسوب می‌شوند، عبارتند از:

- استاندارد ملی ایران شماره ۱۳۲۲۰: سال ۱۳۸۹[4] انفورماتیک سلامت[5]، مدیریت امنیت اطلاعات در بهداشت با استفاده از ISO/IEC 27002

۰-۳ هدف از این استاندارد ملی

این استاندارد ملی، مرور کلی بر سامانه‌های مدیریت امنیت اطلاعات که موضوع استانداردهای خانواده ISMS را شکل می‌دهند، ارائه و اصطلاحات مرتبط را تعریف می‌کند.

یادآوری- در پیوست الف، چگونگی توصیف الزامات و/یا راهنما استانداردهای خانواده ISMS مشخص شده است.

استانداردهای خانواده ISMS شامل استانداردهایی است که:

الف) الزاماتی برای ISMS و صادرکنندگان گواهی چنین سامانه‌هایی تعریف می‌کند؛

ب) پشتیبانی مستقیم، راهنمای تفصیلی و/ یا تفسیر کلی فرآیندها و الزامات طرح- اجرا- بررسی- اقدام (PDCA) [6] را فراهم می‌کند؛

پ) راهنمایی برای ISMS در هر بخش خاص را نشان می‌دهد؛ و

ت) به ارزشیابی انطباق[7] ISMS می‌پردازد.

۱- معادل استاندارد ISO/IEC 27004 استاندارد ملی ایران شماره ۱۴۰۹۶ سال ۱۳۸۹ موجود است

۲- معادل استاندارد ISO/IEC 27007 استاندارد ملی ایران شماره ۲۷۰۰۷ سال ۱۳۹۱ موجود است

3 - ISO/IEC JTC 1
4 - ISO 27799:2008
5 - Health Informatics
6 - Plan-Do-Check-Act
7 - Conformity Assessment

در خصوص اصطلاحات و تعاریف ارائه شده در این استاندارد ملی نکات زیر قابل ذکر است:

اصطلاحات و تعاریف متداول در خانواده استانداردهای ISMS را در برمی‌گیرد.

تمام اصطلاحات و تعاریف به‌کارگرفته شده در استانداردهای خانواده ISMS را در بر نمی‌گیرد.

استانداردهای خانواده ISMS را در تعریف اصطلاحات مورد استفاده خود، محدود نمی‌کند.

استانداردهایی که فقط به پیاده‌سازی کنترل‌های استاندارد ISO/IEC 27002 می‌پردازند و نه به تمام کنترل‌ها، از استانداردهای خانواده ISMS مستثنی شده‌اند.

به منظور بازتاب تغییر وضعیت استانداردهای خانواده ISMS، انتظار می‌رود این استاندارد ملی به طور مداوم و با تواتر بیشتر نسبت به سایر استانداردها به روز شود.

فناوری اطلاعات- فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، تعیین موارد زیر است:

الف) مرور کلی استانداردهای خانواده ISMS؛

ب) مقدمه‌ای بر سامانه‌های مدیریت امنیت اطلاعات؛

پ) توصیف مختصر فرآیند طرح- اجرا- بررسی- اقدام (PDCA)؛

ت) اصطلاحات و تعاریف مورد استفاده در استانداردهای خانواده ISMS؛

این استاندارد ملی در تمامی انواع سازمان‌ها کاربردپذیر است (مانند بنگاه‌های تجاری، دستگاه‌های دولتی، سازمان‌های غیرانتفاعی).

مراجع الزامی[۱]

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

یادآوری- اصطلاحی که در تعریف یا یادآوری دیگری از این بند تعریف شده باشد به صورت برجسته به همراه شماره آن در داخل پرانتز نشان داده می شود. این اصطلاح برجسته می تواند در تعریف توسط توضیح کامل آن جایگزین گردد. برای مثال:

حمله (۲-۴) به عنوان « تلاشی جهت تخریب[۲]، در معرض خطر قرار دادن[۳]، تغییر[۴]، ناتوان سازی[۵]، سرقت[۶] یا دسترسی غیر مجاز[۷] یا استفاده غیر مجاز یک **دارایی**[۸] (۲-۳) تعریف می‌شود»؛

دارایی (۲-۴) به عنوان « هر آنچه که برای سازمان دارای ارزش باشد تعریف می شود».

اگر اصطلاح «**دارایی**» با تعریف آن جایگزین شود:

۱- در این استاندارد ملی مراجع الزامی معرفی نشده است.

2 - Destroy
3 - Expose
4 - Alter
5 - Disable
6 - Steal
7 - Unauthorized Access
8 - Asset

آنگاه **حمله** عبارتست از: «تلاشی جهت تخریب، در معرض خطر قرار دادن، هشداردهی، ناتوان سازی، سرقت یا دسترسی غیر مجاز یا استفاده غیر مجاز هر آنچه که برای سازمان دارای ارزش باشد.

۲-۱

کنترل دسترسی

اطمینان از دسترسی به **دارایی‌ها** (۲-۳) به صورت مجاز و محدود بر اساس الزامات امنیتی و الزامات کسب و کار[1].

۲-۲

پاسخ‌گویی[2]

مسئولیت هر هستار در قبال اقدامات و تصمیماتش.

۲-۳

دارایی

هر آنچه که برای سازمان ارزش دارد.

یادآوری- انواع مختلفی از دارایی‌ها وجود دارند، از جمله:

الف) **اطلاعات** (۲-۱۸)؛

ب) نرم افزار، مانند برنامه‌ی رایانه‌ای؛

پ) دارایی فیزیکی، مانند رایانه؛

ت) خدمات؛

ث) افراد، صلاحیت‌ها، مهارت‌ها و تجارب آن‌ها؛

ج) دارایی‌های نامشهود[3]، مانند وجهه[4] و شهرت.

۲-۴

حمله

تلاش جهت تخریب، افشا، دستکاری، از کار انداختن، سرقت یا دسترسی غیرمجاز یا استفاده غیرمجاز از یک **دارایی** (۲-۳).

1 - Business
2 - Accountability
3 - Intangibles
4 - Image

۲-۵

احراز هویت[1]

ارائه تضمینی که مشخصه ادعاشده هستار درست است.

۲-۶

اصالت[2]

ویژگی که یک هستار همان است که ادعا می‌کند.

۲-۷

دسترس پذیری[3]

ویژگی در دسترس و قابل استفاده بودن، به محض تقاضای یک هستار مجاز.

۲-۸

تداوم کسب و کار[4]

فرآیندها[5] (۲-۳۱) و/ یا **روش‌های اجرایی**[6] (۲-۳۰) برای اطمینان از تداوم عملیات کسب و کار.

۲-۹

محرمانگی[7]

ویژگی در دسترس یا آشکار نبودن اطلاعات برای افراد، هستارها یا **فرآیندهای** (۲-۳۱) غیرمجاز.

۲-۱۰

کنترل[8]

ابزارهای مدیریت **مخاطره**[9] (۲-۳۴) شامل **خط مشی‌ها**[10] (۲-۲۸)، **روش های اجرایی** (۲-۳۰)، **راهنماها**[1] (۲-۱۶)، اقدامات یا ساختارهای سازمانی است که می‌تواند ماهیت اداری، فنی، مدیریتی یا حقوقی داشته باشد.

---

1 - Authentication
2 - Authenticity
3 - Availability
4 - Business continuity
5 - Process
6 - Procedures
7 - Confidentiality
8 - Control
9 - Risk
10 - Policies

یادآوری- کنترل به عنوان مترادفی برای محافظت[2] یا اقدام متقابل[3] نیز استفاده می‌شود.

۲-۱۱

هدف کنترلی[4]

بیانیه‌ای که نتیجه‌ی پیاده‌سازی **کنترل‌ها** (۲-۱۰) را توصیف می‌کند.

۲-۱۲

اقدام اصلاحی[5]

اقدامی که برای از بین بردن علت یک عدم انطباق شناسلیی شده یا سایر شرایط نامطلوب انجام می‌گیرد.

[استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

۲-۱۳

اثربخشی[6]

میزانی که فعالیت‌های برنامه ریزی شده تحقق یافته و نتایج برنامه ریزی شده به دست آمده است.

[استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

۲-۱۴

کارآیی

رابطه بین نتایج حاصل و میزان مطلوبیت استفاده از منابع.

۲-۱۵

رویداد[7]

وقوع مجموعه‌ای ویژه از شرایط

[ISO/IEC Guide 73:2002]

---

1 - Guidelines
2 - Safeguard
3 - Countermeasure
4 - Control Objective
5 - Corrective Action
6 - Effectiveness
7 - Event

۲-۱۶

راهنما[1]

توصیه‌ای درباره‌ی آن چه انتظار می‌رود، که بتوان با انجام آن به هدفی دست یافت.

۲-۱۷

ضربه[2]

تغییر نامطلوب در سطح تحقق اهداف کسب و کار.

۲-۱۸

دارایی اطلاعاتی[3]

دانش یا داده‌ای که برای سازمان ارزش دارد.

۲-۱۹

امنیت اطلاعات[4]

حفظ **محرمانگی** (۲-۹)، **یکپارچگی**[5] (۲-۲۵) و **دسترس‌پذیری** (۲-۷) اطلاعات.

یادآوری- علاوه بر این، سایر ویژگی‌ها، همچون **صحت** (۲-۶)، **پاسخگویی** (۲-۲)، **انکار ناپذیری**[6] (۲-۲۷)، و **قابلیت اطمینان** (۲-۳۳) را نیز می‌تواند دربرگیرد.

۲-۲۰

رویداد امنیت اطلاعات

وقوع یک حالت شناسایی شده از سامانه، خدمت یا شبکه که یک نقض احتمالی از **امنیت اطلاعات** (۲-۱۹) **خط مشی** (۲-۲۸) یا شکست در **کنترل‌ها** (۲-۱۰)، یا موقعیت ناشناخته قبلی که می‌تواند مرتبط با امنیت باشد را نشان می‌دهد.

1 - Guideline
2 - Impact
3 - Information Asset
4 - Information Security
5 - Integrity
6 - Non-repudiation

۲-۲۱

رخداد[1] امنیت اطلاعات

یک یا مجموعه‌ای از **رویدادهای امنیت اطلاعات** (۲-۲۰) ناخواسته یا پیش‌بینی نشده که به احتمال زیاد، عملیات کسب و کار را به خطر می‌اندازد و **امنیت اطلاعات** (۲-۱۹) را تهدید می‌کند.

۲-۲۲

مدیریت رخداد امنیت اطلاعات

فرآیندهایی (۲-۳۱) به منظور آشکارسازی[2]، گزارش‌دهی، ارزشیابی، پاسخ‌دهی به، رسیدگی به و یادگیری از **رخدادهای امنیت اطلاعات** (۲-۲۱).

۲-۲۳

سامانه مدیریت امنیت اطلاعات (ISMS)

قسمتی از **سامانه مدیریت** (۲-۲۶) کلان که مبتنی بر رویکرد مخاطره کسب و کار بوده و به منظور برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازبینی، نگهداری و بهبود **امنیت اطلاعات** (۲-۱۹).

۲-۲۴

مخاطره امنیت اطلاعات

توانایی بالقوه یک **تهدید** (۲-۴۵)، در بهره‌جویی از **آسیب‌پذیری** (۲-۴۶) یک یا گروهی از **دارایی‌ها** (۲-۳) و در نتیجه آسیب زدن به سازمان.

۲-۲۵

یکپارچگی

ویژگی حفاظت از صحت و تمامیت **دارایی‌ها** (۲-۳).

۲-۲۶

سامانه مدیریت

چارچوب **خط‌مشی‌ها** (۲-۲۸)، **روش های اجرایی** (۲-۳۰)، **راهنماها** (۲-۱۶) و منابع مرتبط به منظور دستیابی به اهداف سازمان.

---

1 - Incident
2 - Detection

۲-۲۷

انکار ناپذیری

توانایی اثبات ادعای وقوع **رویداد** (۲-۱۵) یا اقدام و هستارهای آغازکننده‌ی آن، به منظور حل اختلاف درمورد وقوع یا عدم وقوع **رویداد** (۲-۱۵) یا اقدام و دخالت هستارها در **رویداد** (۲-۱۵).

۲-۲۸

خط مشی

نیت و جهت‌گیری کلی که به طور رسمی به وسیله مدیریت تصریح می‌شود.

۲-۲۹

اقدام پیشگیرانه[1]

اقدامی برای از بین بردن علت یک عدم انطباق بالقوه یا سایر شرایط نامطلوب بالقوه انجام می‌گیرد.

[استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

۲-۳۰

روش اجرایی[2]

طریقه ی مشخص شده‌ای برای اجرای[3] یک فعالیت یا یک **فرایند** (۲-۳۱).

[استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

۲-۳۱

فرآیند

مجموعه فعالیت‌های مرتبط با هم یا متعامل که دروندادها را به بروندادها تبدیل می‌کند.

[استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

۲-۳۲

سابقه[4]

مدرکی که در آن نتایج بدست آمده ذکر می شود یا شواهدی را دال بر انجام فعالیت‌ها فراهم می‌آورد.

[استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

---

1 - Preventive Action
2 - Procedure
3 - Carry out
4 - Record

۲-۳۳

قابلیت اطمینان[1]

ویژگی سازگاری با رفتار و نتایج مورد نظر.

۲-۳۴

مخاطره

ترکیبی از احتمال وقوع یک **رویداد** (۲-۱۵) و پیامد آن.

[ISO/IEC Guide 73:2002]

۲-۳۵

پذیرش مخاطره

تصمیم‌گیری در مورد پذیرش یک **مخاطره** (۲-۳۴).

[ISO/IEC Guide 73:2002]

۲-۳۶

تحلیل مخاطره

استفاده‌ی نظام‌مند از اطلاعات به منظور شناسایی منابع و برآورد **مخاطره** (۲-۳۴).

[ISO/IEC Guide 73:2002]

یادآوری- تحلیل مخاطره پایه‌ای را برای **ارزیابی مخاطره** (۲-۴۱)، **بر طرف سازی مخاطره**[2] (۲-۴۳) و **پذیرش مخاطره** (۲-۳۵) فراهم می‌سازد.

۲-۳۷

ارزشیابی مخاطره

فرآیند (۲-۳۱) کلی تحلیل مخاطره (۲-۳۶) و ارزیابی مخاطره (۲-۴۱).

[ISO/IEC Guide 73:2002]

۲-۳۸

اطلاع‌رسانی مخاطره[3]

تبادل یا به اشتراک‌گذاری اطلاعات درباره **مخاطره** (۲-۳۴) بین تصمیم‌گیرنده و سایر ذی‌نفعان.

[ISO/IEC Guide 73:2002]

---

1 - Reliability
2 - Risk treatment
3 - Risk communication

۲-۳۹

معیارهای مخاطره

شرایط مرجع که اهمیت **مخاطره** (۲-۳۴) بر اساس آن‌ها ارزشیابی می‌شود.

[ISO/IEC Guide 73:2002]

۲-۴۰

برآورد مخاطره[1]

فعالیت تخصیص دادن مقدار به احتمال وقوع و پیامدهای **مخاطره** (۲-۳۴).

[ISO/IEC Guide 73:2002]

۲-۴۱

ارزیابی مخاطره

فرآیند (۲-۳۱) مقایسه **مخاطره** (۲-۳۴) برآورد شده با **معیار مخاطره** (۲-۳۹) مفروض به منظور تعیین اهمیت **مخاطره** (۲-۳۴).

[ISO/IEC Guide 73:2002]

۲-۴۲

مدیریت مخاطره[2]

فعالیت‌های هماهنگ به منظور هدایت و کنترل سازمان با توجه به **مخاطره** (۲-۳۴).

[ISO/IEC Guide 73:2002]

یادآوری- مدیریت مخاطره به‌طور کلی شامل **ارزشیابی مخاطره** (۲-۳۷)، **بر طرف سازی مخاطره** (۲-۴۳)، **پذیرش مخاطره** (۲-۳۵)، **اطلاع رسانی مخاطره** (۲-۳۸)، پایش مخاطره و بازنگری مخاطره است.

۲-۴۳

بر طرف سازی مخاطره

فرآیند (۲-۳۱) انتخاب و پیاده‌سازی اقداماتی برای تعدیل **مخاطره** (۲-۳۴).

[ISO/IEC Guide 73:2002]

1 - Risk Estimation
2 - Risk Management

۲-۴۴

بیانیه کاربست‌پذیری[1]

بیانیه مستندی که **اهداف کنترلی** (۲-۱۱) و **کنترل‌های** (۲-۱۰) مرتبط و کاربرد پذیر در **ISMS** (۲-۲۳) سازمان را تشریح می‌کند.

۲-۴۵

تهدید

عامل بالقوه‌ی رخدادی ناخواسته که ممکن است باعث آسیب‌رسانی به سامانه یا سازمان شود.

۲-۴۶

آسیب پذیری

ضعف یک **دارایی** (۲-۳) یا **کنترل** (۲-۱۰) که می‌تواند توسط **تهدید** (۲-۴۵)، مورد بهره‌جویی قرار گیرد.

۳ سامانه‌های مدیریت امنیت اطلاعات

۳-۱ مقدمه

سازمان‌ها از هر نوع و اندازه:

الف) مقدار زیادی اطلاعات را جمع‌آوری، پردازش، ذخیره و ارسال می‌کنند؛

ب) تشخیص می‌دهند که اطلاعات و فرآیندها، سامانه‌ها، شبکه‌ها و افراد مرتبط، دارایی‌های مهمی برای رسیدن به اهداف سازمان هستند؛

پ) با گستره‌ای از مخاطرات مواجه‌اند که ممکن است بر کارکرد دارایی‌ها اثر بگذارند؛ و

ت) با پیاده‌سازی کنترل‌های امنیت اطلاعات، مخاطرات را تعدیل می‌کنند.

تمام اطلاعات نگهداری و پردازش شده توسط سازمان، در معرض تهدیدهای حمله، خطا، عوامل طبیعی (مانند سیل یا آتش سوزی) و غیره قرار دارند و با آسیب‌پذیری‌های ذاتی در کاربرد آنها مواجه هستند. اصطلاح امنیت اطلاعات عموما مبتنی بر اطلاعاتی است که دارایی قلمداد می‌شوند و به علت ارزشی که دارند باید برای مثال در برابر از بین رفتن دسترس‌پذیری، محرمانگی و یکپارچگی، مورد حفاظت مناسب قرار گیرند. دسترسی به موقع به اطلاعات دقیق و کامل از سوی افرادی با نیاز مجاز، باعث تقویت بازدهی کسب و کار می‌شود.

1 - Statement of Applicability

حفاظت از دارایی‌های اطلاعاتی از طریق تعریف، به‌دست آوردن، نگهداری، و بهبود موثر امنیت اطلاعات، برای توانمندسازی سازمان به منظور دستیابی به اهداف و نگهداری و افزایش انطباق قانونی و وجهه‌ی آن ضروری است. این فعالیت‌های هماهنگ که پیاده‌سازی کنترل‌های مناسب را هدایت و مخاطرات امنیت اطلاعات غیر قابل قبول را بر طرف می‌کنند، عموماً اجزای مدیریت امنیت اطلاعات قلمداد می‌شوند.

نظر به اینکه مخاطرات امنیت اطلاعات و اثربخشی تغییر کنترل‌ها وابسته به تغییر وضعیت‌ها است، سازمان‌ها نیاز دارند که:

الف) اثربخشی کنترل‌ها و روش های اجرایی پیاده‌سازی شده را پایش و ارزیابی کنند؛

ب) مخاطرات نوظهوری را که باید بر طرف شوند، شناسایی کنند؛ و

پ) کنترل‌های مناسب مورد نیاز را برگزینند، پیاده‌سازی کنند و بهبود دهند.

به منظور مرتبط و هماهنگ نمودن این‌گونه فعالیت‌های امنیت اطلاعات، هر سازمان باید خط‌مشی و اهداف خود برای امنیت اطلاعات را تعیین نماید و با استفاده از سامانه مدیریت به طور موثری آن اهداف را بدست آورد.

۳-۲ سامانه مدیریت امنیت اطلاعات (ISMS) چیست؟

۳-۲-۱ مرور کلی و اصول

سامانه مدیریت امنیت اطلاعات (ISMS) مدلی را برای برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود حفاظت از دارایی‌های اطلاعاتی به منظور تحقق اهداف کسب و کار فراهم می‌سازد که مبتنی بر ارزشیابی مخاطره و سطوح قابل قبول مخاطره سازمان برای بر طرف‌سازی و مدیریت موثر مخاطرات طراحی شده است.

تحلیل الزامات به منظور حفاظت از دارایی‌های اطلاعاتی و اعمال کنترل‌های مناسب و برای اطمینان از حفاظت لازم از این دارایی‌های اطلاعاتی، به پیاده‌سازی موفقیت‌آمیز ISMS کمک می‌کند. اصول بنیادی زیر نیز به پیاده‌سازی موفقیت‌آمیز ISMS کمک می‌کنند:

الف) آگاهی نسبت به ضرورت امنیت اطلاعات؛

ب) تخصیص مسئولیت برای امنیت اطلاعات؛

پ) تلفیق تعهد مدیریت با منافع ذی‌نفعان؛

ت) تقویت ارزش‌های اجتماعی؛

ث) ارزشیابی مخاطرات جهت اعمال کنترل‌های مناسب برای رسیدن به سطوح قابل قبول مخاطره؛

ج) امنیت لحاظ‌شده به عنوان عنصر ضروری سامانه‌ها و شبکه‌های اطلاعاتی؛

چ) پیشگیری و تشخیص فعال رخدادهای امنیت اطلاعات؛

ح) اطمینان از رویکردی جامع برای مدیریت امنیت اطلاعات؛ و
خ) ارزشیابی مستمر امنیت اطلاعات و اعمال اصلاحات مناسب.

۳-۲-۲ اطلاعات

اطلاعات، دارایی است که همانند سایر دارایی‌های مهم کسب و کار برای فعالیت سازمان ضروری است و در نتیجه نیاز به حفاظت مناسب دارد. اطلاعات را می‌توان به شکل‌های بسیاری ذخیره کرد، از جمله: به شکل دیجیتالی[1] (برای مثال داده‌های ذخیره شده در رسانه نوری یا الکترونیکی)، به شکل فیزیکی (برای مثال بر روی کاغذ) و همچنین اطلاعات نامشهود مانند دانش کارکنان. اطلاعات را می‌توان با روش‌های مختلفی برای مثال با استفاده از پیک، ارتباطات الکترونیکی یا به صورت شفاهی انتقال داد. اطلاعات، به هر شکلی که باشد، یا با هر روشی که انتقال یابد، همیشه به حفاظت مناسب نیاز دارد.

اطلاعات هر سازمان به فناوری ارتباطات و اطلاعات وابسته است. این فناوری عنصری اساسی در هر سازمان است و ایجاد، پردازش، ذخیره سازی، انتقال، حفاظت و از بین بردن اطلاعات را تسهیل می‌کند. با گسترش پیوند جهانی محیط کسب و کار، حفاظت از اطلاعات ضرورت بیشتری پیدا می‌کند، زیرا اکنون اطلاعات در معرض انواع بیشتری از تهدیدها و آسیب‌ها قرار دارد.

۳-۲-۳ امنیت اطلاعات

امنیت اطلاعات دارای سه بعد اصلی است که عبارتند از محرمانگی، دسترس‌پذیری و یکپارچگی. امنیت اطلاعات با هدف اطمینان از موفقیت پایدار و تداوم کسب و کار و در جهت کمینه کردن اثرات، شامل به‌کارگیری و مدیریت معیارهای امنیتی مناسبی است که بازه گسترده‌ای از تهدیدات را مورد توجه قرار می‌دهد.

امنیت اطلاعات با پیاده سازی مجموعه‌ای از کنترل‌های کاربردپذیر به‌دست می‌آید که از طریق فرآیند مدیریت مخاطره انتخاب و با استفاده از ISMS مدیریت می‌شود که شامل خط مشی‌ها، فرآیندها، روش‌های اجرایی، ساختارهای سازمانی، نرم‌افزارها و سخت‌افزارها به منظور حفاظت از دارایی‌های اطلاعاتی شناسایی شده است.

به منظور اطمینان از دستیابی به اهداف معین امنیتی و کسب و کار سازمان، این کنترل‌ها باید تعیین، پیاده‌سازی، پایش، بازنگری و در صورت نیاز بهبود داده شوند. کنترل‌های مرتبط با امنیت اطلاعات باید به صورت تنگاتنگی با فرآیندهای کسب و کار سازمان یکپارچه شده باشند.

1 - Digital

۳-۲-۴ مدیریت

مدیریت شامل فعالیت‌های هدایت، کنترل و بهبود مستمر سازمان در بستر ساختارهای مناسب می‌شود. فعالیت‌های مدیریتی شامل اقدامات، روش‌ها یا شیوه سازمان‌دهی، ساماندهی، هدایت، نظارت و کنترل منابع است. ساختارهای مدیریتی از یک فرد در سازمانی کوچک، تا سلسله مراتب مدیریتی با افرادی بسیار در سازمان‌های بزرگ، گسترش می‌یابد.

از دیدگاه ISMS، مدیریت، نظارت و تصمیم‌گیری‌های لازم برای رسیدن به اهداف کسب و کار از طریق حفاظت از دارایی‌های اطلاعاتی سازمان را در بر می‌گیرد. مدیریت امنیت اطلاعات از طریق تدوین و استفاده از خط‌مشی‌ها، استانداردها، روش‌های اجرایی و راهنماهای امنیتی اظهار می گردد که سپس توسط تمام افراد دست‌اندرکار[1] سازمان در کل سازمان اعمال می‌شود.

یادآوری- اصطلاح مدیریت گاهی به افراد اشاره دارد (برای مثال فرد یا گروهی از افراد با اختیارات و مسئولیت راهبری و کنترل سازمان). اصطلاح مدیریت در این بند به این مفهوم نیست.

۳-۲-۵ سامانه مدیریت

سامانه مدیریت برای رسیدن به اهداف سازمان چارچوبی از منابع را به کار می‌گیرد و شامل ساختار سازمانی، خط‌مشی‌ها، فعالیت‌های برنامه‌ریزی، مسئولیت‌ها، اقدامات، روش‌های اجرایی، فرآیندها و منابع می‌شود.

سامانه مدیریت از لحاظ امنیت اطلاعات، به سازمان اجازه می‌دهد تا:

الف) نیازهای امنیتی مشتریان و سایر ذی‌نفعان را برآورده سازد.

ب) فعالیت‌ها و طرح‌های سازمان را بهبود دهد.

پ) اهداف امنیت اطلاعات سازمان را محقق سازد.

ت) با مقررات، قوانین و الزامات[2] صنفی تطبیق یابد.

ث) دارایی‌های اطلاعاتی را به صورت سازمان‌یافته‌ای مدیریت کند به طوری که بهبود مستمر و سازگاری با محیط و اهداف کنونی سازمان تسهیل شود.

۳-۳ رویکرد فرآیندی[3]

سازمان‌ها باید فعالیت‌های بسیاری را تعیین و مدیریت کنند تا کارکرد موثر و کارآمدی داشته باشند. هر فعالیتی که از منابع استفاده می‌کند، باید مدیریت شود تا تبدیل درون‌دادها به برون‌دادها را با به کارگیری مجموعه‌ای از فعالیت‌های مرتبط و متعامل، که یک فرآیند نیز نامیده می‌شود، ممکن سازد.

---

1 - Individual associated
2 - Mandates
3 - Process Approach

درون‌داد یک فرآیند می‌تواند به طور مستقیم ورودی فرآیند دیگری باشد و عموماً این تبدیل در شرایط کنترل‌شده و برنامه‌ریزی شده صورت می‌گیرد. به کارگیری سامانه‌ای از فرآیندها در یک سازمان، همراه با شناسایی و تعامل این فرآیندها و مدیریت آن‌ها را می‌توان «رویکرد فرآیندی» نامید.

رویکرد فرآیندی ISMS که در استانداردهای خانواده ISMS ارائه شده بر اساس اصول بهره‌برداری پذیرفته شده در استانداردهای سامانه مدیریتی ایزو معروف به فرایند طرح- اجرا- بررسی- اقدام (PDCA) پایه‌ریزی شده است.

الف) **طرح**- تعیین اهداف و طرح‌ریزی (تحلیل موقعیت سازمان، تعیین اهداف کلی و تنظیم اهداف توسعه طرح‌ها برای رسیدن به آن‌ها)؛

ب) **اجرا**- پیاده‌سازی طرح‌ها (عمل به آنچه برای اجرا برنامه‌ریزی شده است)؛

پ) **بررسی**- سنجش نتایج (سنجش/پایش میزان انطباق دست‌آوردها با اهداف برنامه‌ریزی شده)؛

ت) **اقدام**- اصلاح و بهبود فعالیت‌ها (آموختن از اشتباهات به منظور بهبود فعالیت‌ها برای رسیدن به نتایج بهتر).

۳-۴ چرا ISMS مهم است؟

مخاطرات مرتبط با دارایی‌های اطلاعاتی سازمان باید به عنوان قسمتی از ISMS سازمان، نشان داده شوند. رسیدن به امنیت اطلاعات به مدیریت مخاطره نیاز دارد و شامل مخاطرات ناشی از تهدیدهای فیزیکی، انسانی و فناوری مرتبط با تمام اشکال اطلاعات درون سازمانی و مورد استفاده سازمان می‌شوند. انتظار می‌رود پذیرش ISMS، تصمیمی راهبردی برای سازمان باشد و لازم است این تصمیم بر طبق نیازهای سازمان، کاملا یکپارچه، متناسب[1] و به روز شود.

طراحی و پیاده‌سازی ISMS سازمان، تحت تاثیر نیازها و اهداف سازمان، الزامات امنیتی، فرآیندهای کسب و کار به‌کار گرفته شده و اندازه و ساختار سازمان قرار دارد. لازم است در طراحی و بهره‌برداری از ISMS، منافع و الزامات امنیت اطلاعات همه ذی‌نفعان سازمان شامل مشتریان، تأمین‌کنندگان، شرکای تجاری، سهامداران و طرف‌های سوم منعکس شود.

در دنیای به هم پیوسته[2]، اطلاعات و فرآیندها، سامانه‌ها و شبکه‌های مرتبط، دارایی‌های حیاتی کسب و کار را تشکیل می دهند. سازمان‌ها و سامانه‌ها و شبکه‌های اطلاعاتی آنها، با تهدیدهای امنیتی از سوی گستره‌ی وسیعی از منابع شامل تقلب رایانه‌ای[3]، جاسوسی[4]، خرابکاری[1]، تخریب[2]، آتش‌سوزی و سیل

1 - Scaled
2 - Interconnected World
3 - Computer assited fraud
4 - Espionage

روبرو می‌شوند. آسیب زدن به سامانه‌ها و شبکه‌ها اطلاعاتی به علت کدهای مخرب، رخنه‌گری رایانه‌ای و حملات انکار خدمت[3](DoS)، بیش از پیش فراگیر، جاه طلبانه‌تر و به طور فزآینده‌ای پیچیده شده است.

سامانه مدیریت امنیت اطلاعات برای کسب و کارهای هر دو بخش عمومی و خصوصی مهم است. در هر صنعتی، ISMS یک عامل توانمندساز[4] است که از کسب و کار الکترونیکی پشتیبانی می‌کند و برای فعالیت‌های مدیریت مخاطرات ضروری است. اتصال متقابل شبکه‌های عمومی و خصوصی و به اشتراک‌گذاری دارایی‌های اطلاعاتی، دشواری کنترل دسترسی و ساماندهی اطلاعات را افزایش می‌دهد. به علاوه، توزیع افزاره‌های ذخیره‌سازی سیار که حاوی دارایی‌های اطلاعاتی است، می‌تواند اثر بخشی کنترل‌های مرسوم را تضعیف کند. پذیرش استانداردهای خانواده ISMS می‌تواند نشان‌دهنده‌ی توانایی سازمان در به کارگیری اصول امنیت اطلاعات قابل درک متقابل و پایدار، در برابر شرکای تجاری و سایر طرف‌های ذی‌نفع باشد.

در بسیاری موارد امنیت اطلاعات در طراحی و توسعه سامانه‌های اطلاعاتی در نظر گرفته نمی‌شود. به علاوه، امنیت اطلاعات را اغلب راهکاری فنی تلقی می‌کنند. به هر حال، امنیتی که از طریق ابزارهای فنی به دست می‌آید، محدود و ممکن است بدون پشتیبانی مدیریت و روش های اجرایی مناسب در بستر ISMS، بی‌تأثیر باشد. گنجاندن امنیت در سامانه اطلاعاتی پس از پیاده‌سازی آن، کار پرزحمت و پرهزینه‌ای است. ISMS شامل شناسایی کنترل‌های موجود است و به برنامه‌ریزی دقیق و توجه به جزئیات نیاز دارد. برای مثال، کنترل‌های دسترسی که ممکن است فنی (منطقی)، فیزیکی، اداری (مدیریتی) یا ترکیبی از این‌ها باشند، ابزارهایی را فراهم می‌آورد تا از دسترسی مجاز و محدود به دارایی-های اطلاعاتی، مبتنی بر کسب و کار و الزامات امنیتی، اطمینان حاصل شود.

به‌کارگیری موفقیت‌آمیز ISMS برای حفاظت از دارایی‌های اطلاعاتی اهمیت دارد و به سازمان امکان می‌دهد تا:

الف) به اطمینان بیشتری دست یابد که از دارایی‌های اطلاعاتی به میزان کافی و به طور پیوسته در مقابل مخاطرات امنیت اطلاعات حفاظت می‌شود؛

ب) چارچوب ساختاریافته و فراگیری را برای شناسایی و ارزشیابی مخاطرات امنیت اطلاعات، انتخاب و اعمال کنترل‌های کاربردپذیر و سنجش و بهبود اثربخشی آن‌ها داشته باشد؛

پ) محیط کنترل خود را به طور مداوم بهبود دهد؛ و

---

1 - Sabotage
2 - Vandalism
3 - Denial of Service
4 - Enabler

ت) به طور موثر با قوانین و مقررات تنظیم‌شده منطبق شود.

۳-۵ برقراری، پایش، نگه‌داری و بهبود ISMS

۳-۵-۱ مرور کلی

یک سازمان برای برقراری، پایش، نگهداری و بهبود ISMS خود، نیازمند تعهد به انجام مراحل زیر است:

الف) شناسایی دارایی‌های اطلاعاتی و الزامات امنیتی مربوط به آن‌ها (طبق بند ۳-۵-۲)؛

ب) ارزشیابی مخاطرات امنیت اطلاعات (طبق بند ۳-۵-۳)؛

پ) انتخاب و پیاده سازی کنترل‌های مربوطه برای مدیریت مخاطرات غیرقابل پذیرش (طبق بند ۳-۵-۴)؛

ت) پایش، نگهداری و بهبود اثربخشی کنترل‌های امنیتی مربوط به دارایی‌های اطلاعاتی سازمان (طبق بند ۳-۵-۵)؛

برای اطمینان از حفاظت موثر و مستمر ISMS از دارایی‌های اطلاعاتی سازمان ، لازم است مراحل "الف" تا "ت" به طور مداوم جهت شناسایی تغییر در مخاطرات یا در راهبردهای سازمان یا اهداف کسب و کار تکرار شود.

۳-۵-۲ شناسایی الزامات امنیت اطلاعات

الزامات امنیت اطلاعات را می‌توان در محدوده‌ی راهبرد کلی و اهداف کسب و کار سازمان، اندازه و گستره جغرافیایی آن، با درک موارد زیر شناسایی کرد:

الف) دارایی‌های اطلاعاتی شناسایی شده و ارزش آن‌ها؛

ب) نیازهای کسب وکار برای ذخیره سازی و پردازش اطلاعات؛ و

پ) الزامات قانونی، مقررات تنظیم‌شده و قراردادی.

ارزشیابی روش‌مند مخاطرات مرتبط با دارایی‌های اطلاعاتی سازمان، شامل تحلیل تهدیدها علیه دارایی‌های اطلاعاتی؛ آسیب‌پذیری‌ها و احتمال تحقق تهدید در مورد دارایی‌های اطلاعاتی؛ و اثر بالقوه‌ی هر رخداد امنیت اطلاعات بر دارایی‌های اطلاعاتی است. انتظار می‌رود هزینه کنترل‌های امنیتی مربوط متناسب با اثر قابل تصور از تحقق مخاطره بر کسب و کار باشد.

۳-۵-۳ ارزشیابی مخاطرات امنیت اطلاعات

مدیریت مخاطرات امنیت اطلاعات به روشی مناسب برای ارزشیابی و بر طرف سازی مخاطره نیاز دارد که ممکن است شامل برآورد هزینه‌ها و منافع، الزامات قانونی، جنبه‌های اجتماعی، اقتصادی و محیطی، خواسته‌های مورد نظر ذی‌نفعان، اولویت‌ها و سایر ورودی‌ها و متغیرهای متناسب باشد. نتایج ارزشیابی مخاطره امنیت اطلاعات به راهنمایی و تعیین تصمیمات مدیریتی مناسب برای برطرف سازی، به منظور

انجام‌دادن و الویت‌بندی مدیریت مخاطرات امنیت اطلاعات و پیاده‌سازی کنترل‌های امنیتی مناسب برای حفاظت در برابر این مخاطرات کمک خواهد کرد. هدایت لازم برای مدیریت مخاطره امنیت اطلاعات، شامل توصیه‌های ارزشیابی مخاطره، بر طرف سازی مخاطره، پذیرش مخاطره، آگاه‌سازی مخاطره، پایش مخاطره و بازنگری مخاطره در استاندارد ISO/IEC 27005 فراهم شده است.

۳-۵-۴ انتخاب و پیاده سازی کنترل‌های امنیت اطلاعات

به محض این که الزامات امنیت اطلاعات شناسایی و مخاطرات امنیت اطلاعات مربوط به دارایی‌های اطلاعاتی شناسایی شده، تعیین و ارزشیابی (شامل تصمیم‌گیری در مورد بر طرف سازی مخاطرات امنیت اطلاعات) گردید، کنترل‌های مناسب را باید انتخاب و پیاده‌سازی کرد تا از کاهش مخاطرات امنیت اطلاعات به سطح قابل قبول سازمان اطمینان حاصل شود. کنترل‌ها را می‌توان از استاندارد ISO/IEC 27002 ، سایر مجموعه‌های کنترلی مناسب یا کنترل‌های جدیدی که متناسب با نیازهای خاص طراحی شده‌اند، انتخاب کرد. انتخاب کنترل‌های امنیتی به الزامات امنیتی، پذیرش مخاطره امنیت اطلاعات، گزینه‌های بر طرف سازی مخاطره و رویکرد عمومی مورد استفاده‌ی سازمان برای مدیریت مخاطره بستگی دارد . انتخاب و پیاده‌سازی کنترل‌ها می‌تواند در قالب بیانیه کاربردپذیری مستند شود تا به تطبیق الزامات کمک کند.

کنترل‌های مشخص شده در استاندارد ISO/IEC 27002 را بهترین اقدامات قابل اعمال در بیشتر سازمان‌ها قلمداد می‌کنند و به آسانی با سازمان‌های دارای اندازه‌ها و پیچیدگی‌های مختلف منطبق می‌شوند. سایر استانداردهای خانواده ISMS، راهنمایی در مورد انتخاب و به کارگیری کنترل‌های امنیت اطلاعات استاندارد ISO/IEC 27002 برای سامانه مدیریت (استاندارد ISO/IEC27001) فراهم می‌کنند.

۳-۵-۵ پایش، نگهداری و بهبود اثربخشی ISMS

یک سازمان نیاز به نگهداری و بهبود ISMS از طریق پایش و ارزشیابی عملکرد آن براساس خط مشی و اهداف سازمان و گزارش نتایج به مدیریت جهت بازنگری ISMS دارد. این بازنگری ISMS، فراهم‌سازی شواهد اعتبارسنجی[1]، درستی‌سنجی[2] و قابلیت ردگیری اقدامات اصلاحی، پیشگیرانه و بهبوددهنده بر پایه‌ی سوابق این نواحی پایش‌شده، شامل پایش کنترل‌های امنیت اطلاعات را ممکن می‌سازد.

۳-۶ عوامل مهم موفقیت ISMS

عوامل زیادی در پیاده‌سازی موفق ISMS موثر هستند تا به سازمان اجازه رسیدن به اهداف کسب وکار خود را بدهد. نمونه‌هایی مهم این عوامل موفقیت عبارتند از:

1 - Validation
2 - Verification

الف) خط مشی امنیت اطلاعات، اهداف، و فعالیت‌های همسو با اهداف؛

ب) رویکرد و چارچوبی برای طراحی، پیاده سازی، پایش، نگهداری، و بهبود امنیت اطلاعات همساز با فرهنگ سازمانی؛

پ) پشتیبانی و پایبندی مشهود از تمامی سطوح مدیریت به خصوص مدیریت عالی؛

ت) درک الزامات حفاظت دارایی اطلاعاتی که از طریق به‌کارگیری مدیریت مخاطره امنیت اطلاعات به دست آمده است؛ (طبق استاندارد ISO/IEC27005)؛

ث) برنامه‌ی موثر آگاه‌سازی، آموزش های حرفه‌ای و تحصیلی به منظور ارتقای سطح آگاهی کارکنان و سایر طرف‌های مرتبط و تشویق آنها به رعایت الزامات مندرج در خط مشی‌ها و استانداردهای امنیت اطلاعات ؛

ج) فرآیند مدیریت موثر رخداد امنیت اطلاعات؛

چ) رویکرد موثر مدیریت تداوم کسب وکار؛

ح) سامانه سنجش جهت ارزیابی عملکرد مدیریت امنیت اطلاعات و بازخورد پیشنهادهای بهبود عملکرد.

سامانه‌ی مدیریت امنیت اطلاعات (ISMS)، احتمال دستیابی سازمان به عوامل اصلی موفقیت مورد نیاز برای حفاظت دارایی‌های اطلاعاتی را به طور مستمر افزایش می‌دهد.

۳-۷ مزایای استانداردهای خانواده ISMS

مزایای پیاده‌سازی ISMS عمدتاً ناشی از کاهش مخاطرات امنیت اطلاعات (مانند کاهش احتمال و/یا اثر ایجاد شده توسط رخدادهای امنیت اطلاعات) است. مزایای پذیرش استانداردهای خانواده ISMS به طور خاص عبارتند از:

الف) پشتیبانی از فرآیند مشخص‌سازی، پیاده‌سازی، بهره‌برداری و نگهداری یک ISMS یکپارچه و مقرون به صرفه‌ی جامع و منظم که نیازهای سازمان را در بهره‌برداری‌ها و جایگاه‌های مختلف برآورده می‌کند؛

ب) کمک به مدیریت در ساختاربندی رویکردهای مدیریت امنیت اطلاعات در بستر همکاری مدیریت و زمامداری مخاطره، شامل کارآموزی و آموزش صاحبان سامانه و کسب و کار بر اساس مدیریت کلان نگر[1] امنیت اطلاعات؛

پ) ترویج اقدامات امنیت اطلاعات مطلوب و پذیرفته‌شده‌ی جهانی، با روش غیر دستوری و آزادی عمل دادن به سازمان‌ها در پذیرش و بهبود کنترل‌های متناسب با موقعیت‌های خاص آن‌ها به منظور ایستادگی در برابر تغییرات داخلی و خارجی؛ و

1 - Holistic

ت) تدارک زبان مشترک و مفاهیم پایه برای امنیت اطلاعات و ایجاد اطمینان در شرکای کسب وکار نسبت به ISMS مورد توافق، به خصوص اگر در پی دریافت گواهی رعایت استاندارد ISO/IEC27001 از نهاد معتبر صدور گواهی[1] باشند.

۴ استانداردهای خانواده ISMS

۴-۱ اطلاعات کلی

استانداردهای خانواده ISMS شامل استانداردهای مرتبط با هم است که در گذشته منتشر شده‌اند یا در دست تدوین هستند و تعدادی از مولفه‌های ساختاری مهم را در برمی‌گیرند. این مولفه‌ها متمرکز بر استانداردهایی اجباری است که به توصیف الزامات ISMS (استاندارد ISO/IEC27001) و همچنین الزامات نهاد صدور گواهی (استاندارد ISO/IEC27006) می‌پردازند که مراجع صدور گواهی، انطباق با استاندارد ISO/IEC 27001 را گواهی می‌کنند.

سایر استانداردها راهنمایی برای جنبه‌های مختلف پیاده‌سازی ISMS تاکید به فرآیند عمومی، راهنماهای مرتبط با کنترل و راهنمای بخشی خاص را فراهم می‌کند. روابط استانداردهای خانواده ISMS در شکل ۱ نشان داده شده است.

استانداردهایی که برای پشتیبانی مستقیم، تفسیر و/یا راهنمایی تفصیلی در مورد کل فرآیندها و الزامات PDCA مشخص شده در استاندارد ISO/IEC 27001(طبق بند ۴-۳-۱) ارائه شده است، عبارتند از: ISO/IEC 27000 (طبق بند۴-۲-۱)، استاندارد ISO/IEC 27002 (طبق بند۴-۴-۱)، ISO/IEC 27003 (طبق بند۴-۴-۲)، استاندارد ISO/IEC 27004 (طبق بند۴-۴-۳)، استاندارد ISO/IEC 27005 (طبق بند۴-۴-۴) و ISO/IEC 27007 (طبق بند۴-۴-۵).

در استاندارد ISO/IEC 27006 (طبق بند۴-۳-۲)، الزامات مراجع تدارک بیننده گواهینامه‌های ISMS نشان داده شده است. استاندارد ISO/IEC 27011 (طبق بند۴-۵-۱) و استاندارد ISO/IEC27799 (طبق بند۴-۵-۲)، راهنماهای بخش خاص ISMS را نشان می‌دهد.

استانداردهای خانواده ISMS با بسیاری از استانداردهای دیگر ISO و ISO/IEC ارتباط دارند و به صورت زیر قابل طبقه‌بندی و توصیف هستند:

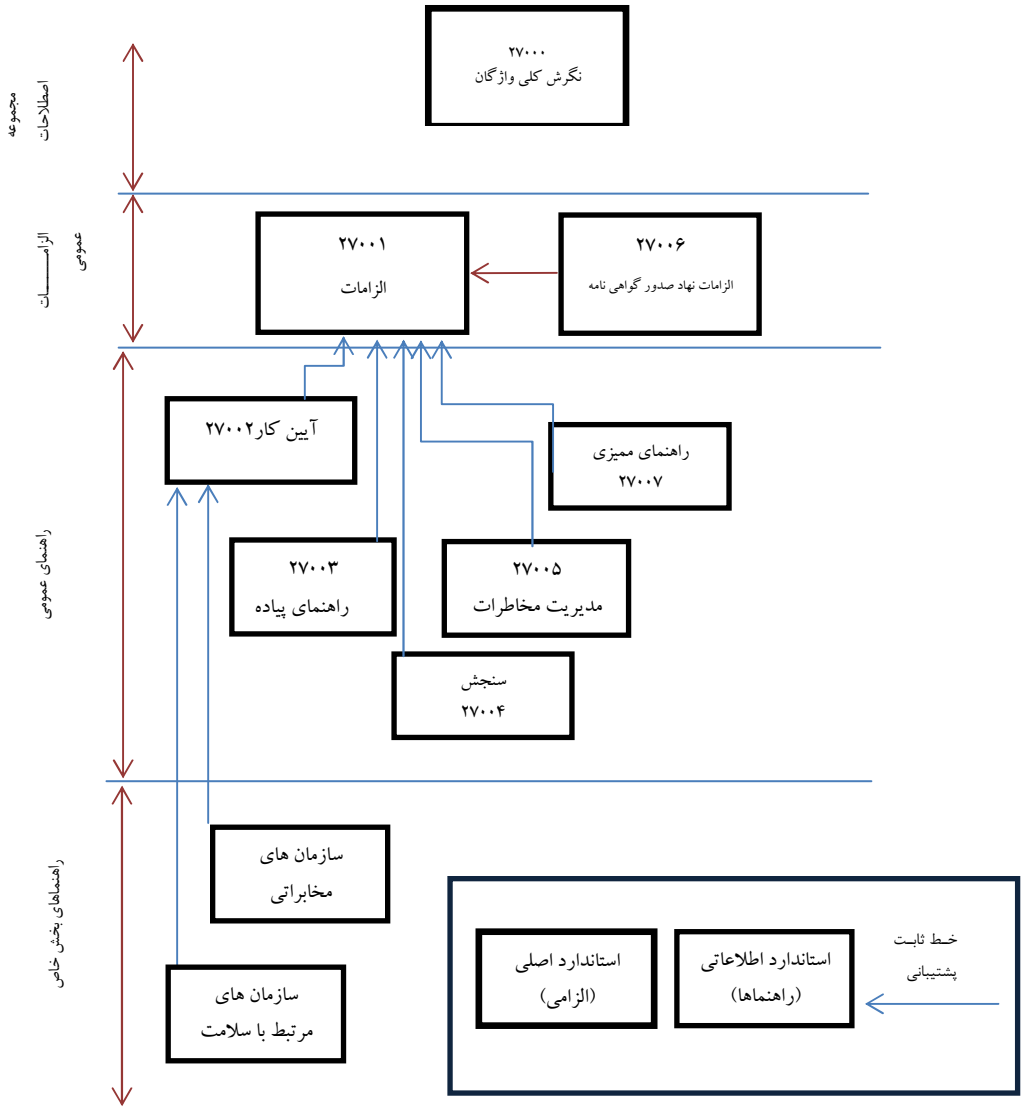
الف) استانداردهای توصیف‌کننده مرور کلی و واژگان (طبق بند۴-۲)؛

ب) استانداردهای مشخص‌کننده الزامات (طبق بند۴-۳)؛

پ) استانداردهای توصیف‌کننده راهنماهای کلی (طبق بند۴-۴)؛ یا

1 - Accredited Certification Body

ت) استانداردهای توصیف‌کننده راهنماهای بخشی خاص (طبق بند۴-۵).



شکل ۱: روابط استانداردهای خانواده ISMS

۴-۲ استانداردهای توصیف کننده مرور کلی و واژگان

۴-۲-۱ ISO/IEC 27000 (سند حاضر)

فناوری اطلاعات- فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان

دامنه کاربرد: این استاندارد ملی موارد زیر را برای سازمان‌ها و افراد فراهم می‌سازد:

الف) مرور کلی بر استانداردهای خانواده ISMS؛

ب) مقدمه‌ای بر سامانه‌های مدیریت امنیت اطلاعات (ISMS)؛

پ) توصیف مختصر فرآیند طرح- اجرا- بررسی- اقدام (PDCA)؛ و

ت) اصطلاحات و تعاریف مورد استفاده در استانداردهای خانواده ISMS.

هدف: ISO/IEC 27000 مبانی سامانه‌های مدیریت امنیت اطلاعات که موضوع استانداردهای خانواده ISMS را شکل می‌دهد توصیف اصطلاحات مرتبط را تعریف می‌کند.

۴-۳ استانداردهای مشخص کننده الزامات

۴-۳-۱ ISO/IEC 27001 [1]

فناوری اطلاعات- فنون امنیتی-سامانه‌های مدیریت امنیت اطلاعات-الزامات

دامنه کاربرد: این استاندارد ملی الزامات برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود سامانه‌های رسمی مدیریت امنیت اطلاعات (ISMS) با درنظرگرفتن محتوای مخاطرات کلی کسب و کار سازمان را مشخص می‌کند. این استاندارد همچنین الزامات پیاده‌سازی کنترل‌های امنیتی تطابق داده شده با نیازهای سازمان‌های مختلف یا بخش‌های وابسته به آن، مشخص شده است. این استاندارد ملی، تمامی انواع سازمان‌ها (مانند بنگاه‌های تجاری، موسسات دولتی، سازمان‌های غیرانتفاعی) را در برمی‌گیرد.

هدف: استاندارد ISO/IEC 27001 الزامات اجباری به منظور توسعه و بهره‌برداری از ISMS را ارائه می‌کند که شامل مجموعه کنترل‌هایی برای مهار و کاهش مخاطرات مرتبط با دارایی‌های اطلاعاتی که سازمان با کمک ISMS حفاظت می‌کند. سازمان‌های بهره‌بردار ISMS ممکن است منطبق با خود، ممیزی و گواهی کنند. اهداف کنترلی و کنترل‌های پیوست الف (استاندارد ISO/IEC 27001) باید به عنوان قسمتی از این فرآیند ISMS انتخاب شوند تا الزامات شناسایی شده را به طور مناسب پوشش دهند. اهداف کنترلی و کنترل‌های فهرست شده در جدول الف-۱ (استاندارد ISO/IEC 27001) به طور مستقیم از بندهای ۵ تا ۱۵ استاندارد ISO/IEC 27002 استخراج شده است و تراز شده بر آن‌ها است.

۴-۳-۲ ISO/IEC 27006 [2]

فناوری اطلاعات- فنون امنیتی – الزامات نهادهای ارائه‌دهنده خدمات ممیزی و صدور گواهی سامانه‌های مدیریت امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی علاوه بر الزامات موجود در ISO/IEC 17021، الزاماتی را مشخص نموده و راهنمایی برای مراجع ارائه‌کننده‌ی ممیزی و گواهی ISMS طبق استاندارد ISO\IEC 27001 را فراهم می‌کند. این استاندارد در اصل برای پشتیبانی از تایید صلاحیت نهادهای گواهی‌کننده‌ای است که گواهی ISMS را طبق استاندارد ISO/IEC 27001 ارائه می‌کنند.

۱معادل با استاندارد بین المللیISO/IEC 27001 استاندارد ملی ایران شماره ۲۷۰۰۱ سال ۱۳۸۷ وجود دارد.

۲معادل با استاندارد بین المللیISO/IEC 27006 استاندارد ملی ایران شماره ۲۷۰۰۶ سال ۱۳۸۷ وجود دارد

هدف: استاندارد ملی ایران شماره ۲۷۰۰۶ متمم ISO/IEC 17021 است که با اعتبار سازمان‌های صدور گواهی الزامات را فراهم می‌سازد. بنابراین به این سازمان‌ها اجازه می‌دهد تا گواهی انطباق مستمر الزامات استاندارد ملی ایران شماره ۲۷۰۰۱را ارائه دهند.

۴-۴ استانداردهای توصیف کننده راهنمای مرور کلی

۱-۴-۴ ISO/IEC 27002 [۱]

فناوری اطلاعات- فنون امنیتی- آیین کار مدیریت امنیت اطلاعات

دامنه کاربرد : این استاندارد ملی، فهرستی از اهداف کنترلی پذیرفته‌شده معمول و کنترل‌های برتر جهت استفاده به عنوان راهنمای پیاده‌سازی در زمان انتخاب و پیاده‌سازی کنترل‌ها برای رسیدن به امنیت اطلاعات را ارائه می‌دهد.

هدف: استاندارد ملی ایران شماره ۲۷۰۰۲ راهنمایی بر پیاده‌سازی کنترل‌های امنیت اطلاعات فراهم می‌آورد. به‌خصوص توصیه‌های مختص پیاده‌سازی در بندهای ۵ تا ۱۵ و راهنمایی راجع به بهترین پشتیبانی از کنترل‌های مشخص‌شده در بندهای الف-۵ تا الف-۱۵ استاندارد ملی ایران شماره ۲۷۰۰۱ را ارائه می‌دهد.

۲-۴-۴ ISO/IEC 27003 [۲]

فناوری اطلاعات- فنون امنیتی- راهنمای پیاده‌سازی سامانه مدیریت امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی، راهنمای پیاده‌سازی عملی است و اطلاعات بیشتری برای برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود ISMS براساس استاندارد ملی ایران شماره ۲۷۰۰۱ را ارائه می‌دهد.

هدف: استاندارد ملی ایران شماره ۲۷۰۰۳ رویکرد فرآیندگرا به پیاده‌سازی موفق ISMS بر اساس استاندارد ملی ایران شماره ۲۷۰۰۱ ارائه خواهد کرد.

۱معادل با استاندارد بین المللیISO/IEC 27002 استاندارد ملی ایران شماره ۲۷۰۰۲ سال ۱۳۸۷ وجود دارد

۲معادل با استاندارد بین المللی ISO/IEC 27003 استاندارد ملی ایران شماره ۲۷۰۰۳ سال ۱۳۸۹ وجود دارد

ISO/IEC 27004 [1] ۳-۴-۴

فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- سنجش

دامنه کاربرد: استاندارد ملی، راهنمایی‌ها و توصیه‌هایی راجع به تدوین و به کارگیری سنجش به منظور ارزشیابی اثربخشی ISMS، اهداف کنترلی و کنترل‌های استفاده شده در پیاده سازی و مدیریت امنیت اطلاعات همانطور که در استاندارد ملی ایران شماره ۲۷۰۰۱ مشخص شده را ارائه خواهد کرد.

هدف: استاندارد ملی ایران شماره ۱۴۰۹۶چارچوبی برای سنجش ارائه کرده که سنجش ارزشیابی اثربخشی ISMS براساس استاندارد ملی ایران شماره ۲۷۰۰۱ را میسر خواهد کرد.

ISO/IEC 27005 [2] ۴-۴-۴

فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی، راهنماهایی برای مدیریت مخاطرات امنیت اطلاعات ارائه می‌کند. رویکرد توصیف‌شده در این استاندارد ملی، مفاهیم کلی مشخص‌شده در استاندارد ملی ایران شماره ۲۷۰۰۱را پشتیبانی می‌کند.

هدف: استاندارد ملی ایران شماره ۲۷۰۰۵ راهنمایی بر پیاده سازی رویکرد مدیریت مخاطرات فرآیندگرا برای کمک به پیاده‌سازی رضایت‌بخش و تحقق الزامات استاندارد ملی ایران شماره ۲۷۰۰۱ برای مدیریت مخاطره امنیت اطلاعات را ارائه می‌دهد.

ISO/IEC 27007 ۵-۴-۴

فناوری اطلاعات- فنون امنیتی- راهنمای ممیزی سامانه‌های مدیریت امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی، افزون بر راهنمایی ارائه شده در استاندارد ملی ایران شماره ۱۹۰۱۱ است که به طور کلی در سامانه‌های مدیریتی کاربردپذیر است، راهنمایی را بر انجام ممیزی ISMS و نیز راهنمایی بر صلاحیت ممیزان سامانه مدیریت امنیت اطلاعات ارائه خواهد داد.

هدف: ISO/IEC 27007 راهنمایی برای سازمان‌هایی که نیاز به انجام ممیزی داخلی یا خارجی ISMS دارند یا برنامه ممیزی ISMS را در برابر الزامات مشخص شده در استاندارد ملی ایران شماره ۲۷۰۰۱ مدیریت می‌کنند، فراهم خواهد کرد.

۱معادل با استاندارد بین المللی ISO/IEC 27004 استاندارد ملی ایران شماره ۱۴۰۹۶سال ۱۳۸۹ وجود دارد

۲معادل با استاندارد بین المللی ISO/IEC 27005 استاندارد ملی ایران شماره ۲۷۰۰۵ سال ۱۳۸۸ وجود دارد

۴-۵ استانداردهای توصیف کننده راهنماهای بخش خاص

۴-۵-۱ ISO/IEC 27011 [1]

فناوری اطلاعات- فنون امنیتی- راهنماهای مدیریت امنیت اطلاعات برای سازمان‌های مخابراتی بر پایه استاندارد ملی ایران شماره ۲۷۰۰۲

دامنه کاربرد: این استاندارد ملی، راهنماهای پشتیبانی‌کننده از پیاده‌سازی مدیریت امنیت اطلاعات (ISM) در سازمان‌های مخابراتی را ارائه می‌کند.

هدف: استاندارد ملی ایران شماره ۲۷۰۱۱، برای سازمان‌های مخابراتی، با پذیرش راهنماهای منحصر به فرد استاندارد ملی ایران شماره ۲۷۰۰۲ در بخش صنعت آن‌ها که افزون بر راهنمای ارائه شده نسبت به تحقق الزامات پیوست الف استاندارد ملی ایران شماره ۲۷۰۰۱ است را ارائه می‌کند.

۴-۵-۲ ISO 27799 [2]

انفورماتیک سلامت- مدیریت امنیت اطلاعات در سلامت با استفاده از استاندارد ملی ایران شماره ۲۷۰۰۲

دامنه کاربرد: این استاندارد ملی، راهنماهای پشتیبانی کننده از پیاده‌سازی مدیریت امنیت اطلاعات (ISM) در سازمان‌های بهداشت را ارائه می‌کند.

هدف: استاندارد ملی ایران شماره ۱۳۲۲۰، برای سازمان‌های سلامت، با پذیرش راهنماهای منحصر به فرد استاندارد ملی ایران شماره ۲۷۰۰۲ در بخش صنعت آن‌ها که افزون بر راهنمای ارائه شده نسبت به تحقق الزامات پیوست الف استاندارد ملی ایران شماره ۲۷۰۰۱ است را ارائه می‌کند.

۱معادل با استاندارد بین المللی ISO/IEC 27011 استاندارد ملی ایران شماره ۲۷۰۱۱ سال۱۳۸۹ وجود دارد

۲معادل با استاندارد بین المللی ISO 27799 استاندارد ملی ایران شماره ۱۳۲۲۰ سال ۱۳۸۹ وجود دارد

پیوست الف

(اطلاعاتی)

کاربرد افعال در بیان مقررات

هر کدام از مستندات استانداردهای خانواده ISMS به خودی خود تعهدی برای کسی ایجاد نمی‌کند. اما چنین تعهدی برای مثال ممکن است توسط مقررات یا قراردادی ایجاد شود. برای آن که کاربر بتواند ادعای انطباق با سندی را داشته باشد، باید الزامات را شناسایی کند. همچنین در مواردی که آزادی انتخاب وجود دارد، کاربر باید بتواند این الزامات را از سایر توصیه‌ها تشخیص دهد.

جدول زیر چگونگی تفسیر اصطلاح کاربرد افعالی که می‌تواند الزامات و/یا توصیه‌ها برای مستندات استانداردهای خانواده‌ی ISMS باشد را تصریح می‌کند.

نشانه	شرح
الزامات[a]	اصطلاحات «باید[b]» و «نباید[c]» دلالت بر الزاماتی دارد که به شدت دنبال می‌شوند تا مطابق با سند باشد و انحراف از آن مجاز نیست.
توصیه[d]	اصطلاحات «توصیه می‌شود[e]» و «توصیه نمی‌شود[f]» نشان دهنده این است که از میان چندین مورد محتمل، یک مورد خصوصا، مناسب است، بدون آن که به گزینه‌های دیگر اشاره یا آن‌ها را مستثنی کند یا این که عمل معینی برتری داده شود ولی نه لزوماً الزامی بوده یا که (به شکل منفی آن) احتمال یا عمل معینی ناچیز انگاشته شود ولی منع نشود.
اجازه[g]	اصطلاح «مجاز است[h]» و «نیازی نیست[i]» نشان می‌دهد که یک عمل در محدوده سند مجاز است.
امکان[j]	اصطلاح «می‌توان[k]» و «نمی‌توان[l]» نشان دهنده احتمال وقوع چیزی است.

[a] Requirement
[b] Shall
[c] Shallnot
[d] Recommendation
[e] Should
[f] Shouldnot
[g] Premission
[h] May
[i] Neednot
[j] Possibility
[k] Can
[l] Cannot

پیوست ب

(اطلاعاتی)

اصطلاحات دسته‌بندی‌شده

ب-۱ اصطلاحات مربوط به امنیت اطلاعات

۲-۲ پاسخ‌گویی	accountability
۲-۵ احراز هویت	authentication
۲-۶ صحت	authenticity
۲-۷ دسترس‌پذیری	availability
۲-۹ محرمانگی	confidentiality
۲-۱۹ امنیت اطلاعات	information security
۲-۲۵ یکپارچگی	integrity
۲-۲۷ انکار ناپذیری	non-repudiation
۲-۳۳ قابلیت اطمینان	reliability

ب-۲ عبارات مربوط به مدیریت

۲-۸ تداوم کسب وکار	business continuity
۲-۱۲ اقدام اصلاحی	corrective action
۲-۱۳ اثربخشی	effectiveness
۲-۱۴ کارایی	efficiency
۲-۱۶ راهنما	guideline
۲-۲۳ سامانه مدیریت امنیت اطلاعات (ISMS)	information security management system (ISMS)
۲-۲۶ سامانه مدیریت	management system
۲-۲۸ خط مشی	policy
۲-۲۹ اقدام پیشگیرانه	preventive action
۲-۳۱ فرآیند	process

ب-۳ عبارات مربوط به مخاطره امنیت اطلاعات

۲-۱ کنترل دسترسی	access control
۲-۳ دارایی	asset
۲-۴ حمله	attack

control	۲-۱۰ کنترل
control objective	۲-۱۱ هدف کنترلی
event	۲-۱۵ رویداد
impact	۲-۱۷ اثر
information asset	۲-۱۸ دارایی اطلاعاتی
information security event	۲-۲۰ رویداد امنیت اطلاعات
information security incident	۲-۲۱ رخداد امنیت اطلاعات
information security incident management	۲-۲۲ مدیریت رخداد امنیت اطلاعات
information security risk	۲-۲۴ مخاطره امنیت اطلاعات
risk	۲-۳۴ مخاطره
risk acceptance	۲-۳۵ پذیرش مخاطره
risk analysis	۲-۳۶ تحلیل مخاطره
risk assessment	۲-۳۷ ارزشیابی مخاطره
risk communication	۲-۳۸ اطلاع رسانی مخاطره
risk criteria	۲-۳۹ معیارهای مخاطره
risk estimation	۲-۴۰ برآورد مخاطره
risk evaluation	۲-۴۱ ارزیابی مخاطره
risk management	۲-۴۲ مدیریت مخاطره
risk treatment	۲-۴۳ بر طرف سازی مخاطره
threat	۲-۴۵ تهدید
vulnerability	۲-۴۶ آسیب پذیری
	ب-۴ عبارات مربوط به مستندسازی
procedure	۲-۳۰ روش اجرایی
record	۲-۳۲ سابقه
statement of applicability	۲-۴۴ بیانیه کاربست پذیری

کتابنامه

[1] ISO/IEC 17021:2006, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[۲] استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷، سیستم های مدیریت کیفیت - مبانی و واژگان

[۳] استاندارد ملی ایران شماره ۱۹۰۱۱: سال ۱۳۸۶، رهنمودهایی برای ممیزی سیستم های مدیریت کیفیت و /یا زیست محیطی

[۴] استاندارد ملی ایران شماره ۲۷۰۰۱ : سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستم های مدیریت امنیت اطلاعات – الزامات

[۵] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستمهای مدیریت امنیت اطلاعات – آیین کار مدیریت امنیت اطلاعات

[6] ISO/IEC 270034), *Information technology — Security techniques — Information security management system implementation guidance*

[7] ISO/IEC 270045), *Information technology — Security techniques — Information security management —Measurement*

[۸] استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۸۸، فناوری اطلاعات – فنون امنیتی – مدیریت ریسک امنیت اطلاعات

[۹] استاندارد ملی ایران شماره ۲۷۰۰۶: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – الزامات نهادهای ممیزی کننده و گواهی کننده سیستم های مدیریت امنیت اطلاعات

[10] ISO/IEC 270076), *Information technology — Security techniques — Guidelines for information security management systems auditing*

[11] ISO/IEC 270117), *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[12] ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

[13] ISO/IEC Guide 73:2002, *Risk Management — Vocabulary — Guidelines for use in standards*