استاندارد ملی ایران-ایزو-
آی ای سی
۲۷۰۰۰
تجدیدنظر اول
۱۳۹۴

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

INSO-ISO-IEC
27000
1st.Revision
2015

فناوری اطلاعات- فنون امنیتی- سیستم‌های (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-سامانه های(سیستم‌های) مدیریت امنیت اطلاعات- مرورکلی وواژگان»

رئیس:	**سمت و/ یا نمایندگی:**
مرتضوی، محمود (دکترا مهندسی نرم‌افزار)	مدیرفنی شرکت پردازشگران داده آرای سپاهان
دبیر:	
میر اسکندری، سید محمدرضا (کارشناسی ارشد مدیریت اجرایی)	مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء:(به ترتیب حروف الفبا)	
ایزدپناه، سحرالسادات (کارشناسی ارشد مهندسی فناوری اطلاعات، سیستم-های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
بهبهانی، فرید (کارشناسی مکانیک، طراحی جامدات)	مدیر عامل شرکت اینفو امن
تیموری، حسین (کارشناسی ارشد مدیریت تکنولوژی، انتقال تکنولوژی)	مدیرعامل نمایندگی شرکت niscert
سجادیه، سید علیرضا (کارشناسی ارشد مهندسی کامپیوتر، هوش مصنوعی و رباتیک)	مدیرعامل شرکت پردازشگران داده آرای سپاهان
طی نیا، رضا (کارشناسی ارشد فناوری اطلاعات، مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
عزیزی پور، محسن (کارشناسی ارشد مدیریت بازرگانی، بازاریابی)	مدیرعامل شرکت پارس آوان رایان
قسمتی، سیمین (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران

کیامهر، بیتا (کارشناسی ارشد مدیریت تکنولوژی)	معـاون مـدیرکل نظـام مـدیریت امنیـت اطلاعـات سـازمان فناوری اطلاعات ایران
محمودی، یعقوب (کارشناسی ارشد فناوری اطلاعات، سیستم‌های اطلاعاتی)	کارشناس رسمی دادگستری
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعـات سازمان فناوری اطلاعات ایران
مهدوی اردستانی، علیرضا (کارشناسی ارشد مدیریت فناوری اطلاعات، سیسـتم-های اطلاعاتی پیشرفته)	رییس هیأت مدیره شرکت داده پردازان آبشار
میرمعینی، علیرضا (کارشناسی ارشد مهندسی صنایع،)	مدیرعامل پژوهش های راهبردی امن رای

فهرست مندرجات

عنوان		صفحه
آشنایی با سازمان ملی استاندارد ایران		ب
کمیسیون فنی تدوین استاندارد		ج
پیش‌گفتار		ز
۰	مقدمه	ح
۰-۱	مرور کلی	ح
۰-۲	استانداردهای خانواده ISMS	ح
۰-۳	هدف از این استاندارد ملی	ی
۱	هدف و دامنه کاربرد	۱
۲	اصطلاحات و تعاریف	۱
۳	سیستم‌های مدیریت امنیت اطلاعات	۱۹
۳-۱	مقدمه	۱۹
۳-۲	سیستم مدیریت امنیت اطلاعات (ISMS) چیست؟	۲۰
۳-۲-۱	مرورکلی و اصول	۲۰
۳-۲-۲	اطلاعات	۲۰
۳-۲-۳	امنیت اطلاعات	۲۱
۳-۲-۴	مدیریت	۲۱
۳-۲-۵	سیستم مدیریت	۲۱
۳-۳	رویکرد فرآیندی	۲۲
۳-۴	چرا ISMS مهم است؟	۲۲
۳-۵	استقرار، پایش، نگهداری و بهبود ISMS	۲۴
۳-۵-۱	مرور کلی	۲۴
۳-۵-۲	شناسایی الزامات امنیت اطلاعات	۲۴
۳-۵-۳	ارزیابی مخاطرات امنیت اطلاعات	۲۴
۳-۵-۴	برطرف‌سازی مخاطرات امنیت اطلاعات	۲۵
۳-۵-۵	انتخاب و پیاده‌سازی کنترل‌ها	۲۶
۳-۵-۶	پایش، نگهداری و بهبود اثربخشیISMS	۲۷
۳-۵-۷	بهبود مستمر	۲۷
۳-۶	عوامل مهم موفقیت ISMS	۲۸
۳-۷	مزایای استانداردهای خانواده ISMS	۲۸
۴	استانداردهای خانواده ISMS	۲۹

۴-۱ اطلاعات کلی ۲۹
۴-۲ استانداردهای توصیف‌کننده مرورکلی و واژگان ۳۲
۴-۲-۱ استاندارد ISO/IEC 27000 (این سند) ۳۲
۴-۳ استانداردهای مشخص‌کننده الزامات ۳۲
۴-۳-۱ استانداردISO/IEC 27001 ۳۲
۴-۳-۲ استانداردISO/IEC 27006 ۳۳
۴-۴ استانداردهای توصیف‌کننده راهنماهای کلی ۳۳
۴-۴-۱ استاندارد ISO/IEC 27002 ۳۳
۴-۴-۲ استانداردISO/IEC 27003 ۳۳
۴-۴-۳ استاندارد ISO/IEC 27004 ۳۴
۴-۴-۴ استانداردISO/IEC 27005 ۳۴
۴-۴-۵ استاندارد ISO/IEC 27007 ۳۴
۴-۴-۶ استاندارد ISO/IEC TR27008 ۳۵
۴-۴-۷ استاندارد ISO/IEC 27013 ۳۵
۴-۴-۸ استاندارد ISO/IEC 27014 ۳۵
۴-۴-۹ استاندارد ISO/IEC TR 27016 ۳۶
۴-۵ استانداردهای توصیف‌کننده راهنماهای بخش خاص ۳۶
۴-۵-۱ استاندارد ISO/IEC 27010 ۳۶
۴-۵-۲ استاندارد ISO/IEC 27011 ۳۶
۴-۵-۳ استاندارد ISO/IEC TR 27015 ۳۷
۴-۵-۴ استاندارد ISO 27799 ۳۷
پیوست الف (اطلاعاتی) کاربرد افعال در بیان مقررات ۳۸
پیوست ب (اطلاعاتی) اصطلاح و مالکیت اصطلاح ۳۹
پیوست پ (اطلاعاتی) واژگان برحسب شماره بندها ۵۲
پیوست ت (اطلاعاتی) واژگان فارسی به انگلیسی ۵۷
پیوست ث (اطلاعاتی) واژگان انگلیسی به فارسی ۶۴
کتاب‌نامه ۷۱

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی-سامانه های (سیستم[1]های) مدیریت امنیت اطلاعات- مرورکلی و واژگان » اولین بار در سال ۱۳۹۱ تدوین شد. این استاندارد بر اساس پیشنهادهای رسیده و بررسی توسط سازمان فناوری اطلاعات ایران و تأیید کمیسیون‌های مربوط برای اولین بار مورد تجدیدنظر قرار گرفت و در سیصد و هفتاد و نهمین اجلاس کمیته ملی فناوری اطلاعات مورخ ۱۳۹۴/۰۵/۰۵ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه 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 زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره INSO-ISO-IEC 27000: سال ۱۳۹۱ است.

منابع و مأخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیراست:

ISO/IEC 27000:2014, Information technology - Security techniques - Information security management systems - Overview and vocabulary

۱- در این استاندارد، از لغت سیستم به جای سامانه برای نام گذاری این استاندارد استفاده شده است.

۰ مقدمه

۰-۱ مرور کلی

استانداردهای ملی سیستم‌های مدیریت، به‌منظور فراهم آوردن مدلی برای استقرار و بهره‌برداری[1] از سیستم مدیریت تهیه‌شده است.این مدل دربردارندهٔ مشخصه‌هایی است که متخصصان این حوزه در مورد آن‌ها به‌عنوان فناوری بین‌المللی روز به اجماع رسیده‌اند. کمیته فرعی ISO/IEC JTC 1/SC 27[2]، شامل گروهی تخصصی است که به تدوین استانداردهای سیستم‌های مدیریت بین‌المللی امنیت اطلاعات می‌پردازد. این استانداردها به‌عنوان استانداردهای خانواده سیستم مدیریت امنیت اطلاعات (ISMS)[3] شناخته می‌شوند.

سازمان‌ها می‌توانند با استفاده از استانداردهای خانواده ISMS، چارچوبی را برای مدیریت امنیت دارایی‌های اطلاعاتی خود شامل اطلاعات مالی[4]، مالکیت معنوی[5]، جزئیات اطلاعات کارکنان[6] یا اطلاعات سپرده‌شده به آن‌ها توسط مشتریان یا طرف‌های سوم[7]تدوین و پیاده‌سازی کنند. این استانداردها می‌توانند برای ارزیابی[8] مستقل سیستم مدیریت امنیت اطلاعات سازمان‌ها، به‌منظور حفاظت از اطلاعات به کار گرفته شوند.

۰-۲ استانداردهای خانواده ISMS

استانداردهای خانواده ISMS (طبق بند ۴) برای کمک به سازمان‌ها از هر نوع و اندازه، به‌منظور پیاده‌سازی و بهره‌برداری از ISMS در نظر گرفته‌شده است و شامل استانداردهای بین‌المللی زیر، با عنوان عمومی فناوری اطلاعات- فنون امنیتی است (به ترتیب عددی ارائه‌شده است):

- ISO/IEC 27000[9] ، سیستم‌های مدیریت امنیت اطلاعات - مرورکلی و واژگان
- ISO/IEC 27001[10] ، سیستم‌های مدیریت امنیت اطلاعات - الزامات
- ISO/IEC 27002[11] ، آیین کار کنترل[12]های امنیت اطلاعات
- ISO/IEC 27003[1] ، راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات

---

1 - Operating
2 - Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) SubCommittee 27
3 - Information Security Management Systems
4 - Financial Information
5 - Intellectual Property
6 - Employee Details
7 - Third Parties
8 - Assessment

۹ - همین استاندارد مورد نظر است.

۱۰- استاندارد ملی ایران با شماره ایزو – آی ای سی ۲۷۰۰۱ در سال ۱۳۸۷ با منبع بین‌المللی ISO/IEC 27001:2005 منتشر شده است.

۱۱- استاندارد ملی ایران با شماره ایزو – آی ای سی ۲۷۰۰۲ در سال ۱۳۸۷با منبع بین‌المللی ISO/IEC 27002:2005 منتشر شده است.

۱۲- فرهنگستان زبان و ادب فارسی، استفاده از واژه واپایش را به جای کنترل پیشنهاد کرده است.

- ISO/IEC 27004[۲] ، مدیریت امنیت اطلاعات- سنجش
- ISO/IEC 27005[۳] ، مدیریت مخاطرات امنیت اطلاعات
- ISO/IEC 27006[۴] ، الزامات نهادهای ارائه‌دهندهٔ خدمات ممیزی و صدور گواهینامه‌های مدیریت امنیت اطلاعات
- ISO/IEC 27007[۵]، راهنمای ممیزی سیستم‌های مدیریت امنیت اطلاعات
- ISO/IEC TR 27008[۶]، راهنمای ممیزان جهت کنترل‌های امنیت اطلاعات
- ISO/IEC 27010[۷]، مدیریت امنیت اطلاعات ارتباطات بین بخشی و بین سازمانی
- ISO/IEC 27011[۸]، راهنمای مدیریت امنیت اطلاعات برای سازمان‌های مخابراتی مبتنی بر ISO/IEC 27002
- ISO/IEC 27013[۹]، راهنمایی در مورد پیاده‌سازی یکپارچه ISO/IEC 27001 و ISO/IEC 20000-1
- ISO/IEC 27014[۱۰]، حاکمیت امنیت اطلاعات
- ISO/IEC TR 27015[۱۱]، راهنمای مدیریت امنیت اطلاعات برای خدمات مالی

۱- استاندارد ملی ایران با شماره ۲۷۰۰۳ ISIRI-ISO-IEC در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27003:2010 منتشر شده است.

۲- استاندارد ملی ایران با شماره ۱۴۰۹۶ ISIRI-ISO-IEC در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27004:2009 منتشر شده است.

۳- استاندارد ملی ایران با شماره ۲۷۰۰۵ INSO -IEC در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27005:2011 منتشر شده است.

۴- استاندارد ملی ایران با شماره ۲۷۰۰۶ ISIRI-ISO-IEC در سال ۱۳۸۷ با منبع بین‌المللی ISO/IEC 27006:2007 منتشر شده است.

۵- استاندارد ملی ایران با شماره ۲۷۰۰۷ INSO-ISO-IEC در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27007:2011 منتشر شده است.

۶- استاندارد ملی ایران با شماره ۲۷۰۰۸ INSO -IEC-TR در سال ۱۳۹۱ با منبع بین‌المللی ISO/IEC 27008:2011 منتشر شده است.

۷- استاندارد ملی ایران با شماره ۲۷۰۱۰ INSO-ISO-IEC در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27010:2012 منتشر شده است.

۸- استاندارد ملی ایران با شماره ۲۷۰۱۱ ISIRI-ISO-IEC در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27011:2008 منتشر شده است.

۹- استاندارد ملی ایران با شماره ۲۷۰۱۳ ISIRI-ISO-IEC در سال ۱۳۹۳ با منبع بین‌المللی ISO/IEC 27013:2012 منتشر شده است.

۱۰- استاندارد ملی ایران با شماره ۲۷۰۱۴ INSO-ISO-IEC در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27014:2013 منتشر شده است.

۱۱- استاندارد ملی ایران با شماره ۲۷۰۱۵ INSO-ISO-IEC-TR در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27015:2012 منتشر شده است.

– ISO/IEC TR 27016[1]، مدیریت امنیت اطلاعات - اقتصاد سازمانی

یادآوری–عنوان عمومی «فناوری اطلاعات- فنون امنیتی» نشان می‌دهد این استانداردها توسط کمیته مشترک فرعی ۲۷ با نام فنون امنیتی فناوری اطلاعات از کمیته فنی مشترک شماره یک ISO/IEC[2] موسوم به فناوری اطلاعات، تدوین‌شده است.

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

– ISO 27799:2008[3] ، انفورماتیک سلامت- مدیریت امنیت اطلاعات در بهداشت با استفاده از ISO/IEC 27002

۰-۳ هدف از این استاندارد ملی

این استاندارد ملی، مرورکلی بر سیستم‌های مدیریت امنیت اطلاعات ارائه کرده و اصطلاحات مرتبط را تعریف می‌کند.

یادآوری–در پیوست الف، چگونگی توصیف الزامات و/یا راهنمای استانداردهای خانواده ISMS مشخص‌شده است.

استانداردهای خانواده ISMS شامل استانداردهایی است که:

الف- الزاماتی برای ISMS و صادرکنندگان گواهی چنین سیستم‌هایی تعریف می‌کند؛

ب- پشتیبانی مستقیم، راهنمای تفصیلی و/یا تفسیر کلی فرآیندها جهت استقرار، پیاده‌سازی،نگهداری و بهبود ISMS را فراهم می‌کند؛

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

ت- به ارزیابی انطباق[4] ISMS می‌پردازد.

در خصوص اصطلاحات و تعاریف ارائه‌شده در این استاندارد ملی نکات زیر وجود دارد:

- اصطلاحات و تعاریف متداول در خانواده استانداردهایISMS را در برمی‌گیرد؛
- تمام اصطلاحات و تعاریف به‌کارگرفته شده در استانداردهای خانواده ISMS را دربرنمی‌گیرد؛ و
- استانداردهای خانواده ISMS را در تعریف اصطلاحات مورد استفاده خود، محدود نمی‌کند.

۱- استاندارد ملی ایران با شماره ۲۷۰۱۶ INSO-ISO-IEC-TR در سال ۱۳۹۳ با منبع بین‌المللی ISO/IEC 27016:2014 منتشر شده است.

2 -ISO/IEC JTC 1

۳- استاندارد ملی ایران با شماره ISIRI۱۳۲۲۰ در سال ۱۳۸۹ با منبع بین المللی ISO 27799:2008 انفورماتیک سلامت، منتشر شده است.

4 - Conformity Assessment

فناوری اطلاعات- فنون امنیتی- سامانه های (سیستم‌های) مدیریت امنیت اطلاعات- مرورکلی و واژگان

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و راهنمائی برای مرور کلی بر سیستم‌های مدیریت امنیت اطلاعات و اصطلاحات و تعاریف که به صورت عمومی مورد استفاده در خانواده استانداردهای ISMS است. این استاندارد در تمامی انواع سازمان‌ها در هر اندازه ای[1] کاربردپذیر است (مانند بنگاه‌های تجاری[2]، دستگاه‌های دولتی[3]، سازمان‌های غیرانتفاعی[4]).

یادآوری – دراین استاندارد ملی مراجع الزامی معرفی نشده است.

۲ اصطلاحات و تعاریف

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

۱-۲

کنترل دسترسی

حصول اطمینان از اینکه دسترسی به دارایی‌ها به‌صورت مجاز و محدود بر اساس الزامات امنیتی و الزامات کسب‌وکار است.

۲-۲

مدل تحلیلی

الگوریتم یا محاسبه‌ای که یک یا چندین سنجه مبنا[5] (۲-۱۰) و/یا سنجه‌های مشتق[6] (۲-۲۲) را با معیار تصمیم‌گیری[7] مرتبط، ترکیب می‌کند.

۳-۲

حمله

تلاشی جهت تخریب، افشا، دست‌کاری، از کار انداختن، سرقت یا دسترسی غیرمجاز یا استفاده غیرمجاز از یک دارایی است.

1- All types and sizes
2 - Commercial enterprises
3 - Government agencies
4 - Notfor-profit organizations
5- Base measures
6- Derived measures
7- Decision criteria

۴-۲

صفت

خصوصیت یا مشخصهٔ شی (۲-۵۵) که به‌صورت کیفی یا کمّی توسط انسان یا ابزارهای خودکار[1] قابل‌تشخیص است.

[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵: سال ۱۳۸۷، تغییریافته- در تعریف، هستار با شی جایگزین شده است.]

۵-۲

ممیزی

فرآیندی (۲-۶۱) نظام‌مند، مستقل و مستند جهت کسب و ارزشیابی هدفمند شواهد عینی ممیزی، به‌منظور تعیین میزان برآورده شدن معیارهای ممیزی است.

یادآوری ۱- ممیزی می‌تواند، ممیزی داخلی (اول شخص) یا خارجی (دوم یا سوم شخص) باشد و همچنین می‌تواند ممیزی ترکیبی باشد (ترکیبی از دو یا چندین نظام).

یادآوری ۲- «شواهد ممیزی» و «معیارهای ممیزی» در ISO 19011 تعریف شده است.

۶-۲

محدوده ممیزی

گستره و مرزهای ممیزی (۲-۵) است.

[منبع:استاندارد ملی ایران شماره ۱۹۰۱۱:سال ۱۳۹۲]

۷-۲

اصالت‌سنجی

کسب اطمینان از آنکه مشخصهٔ ادعاشده هستار، درست است.

۸-۲

اصالت

خصوصیتی که یک هستار، همان است که ادعا می‌کند.

۹-۲

دسترس‌پذیری

خصوصیت در دسترس و قابل‌استفاده بودن، به‌محض تقاضای یک هستار مجاز است.

1- Automated

۱۰-۲

سنجه مبنا

سنجه‌ای (۲-۴۷) است که برحسب یک صفت (۲-۴) و روش کمّی کردن آن تعریف‌شده است.

[منبع:استاندارد ملی ایران شماره ۱۲۷۵۵:سال ۱۳۸۷]

یادآوری ۱- هر سنجه مبنا، ازلحاظ کارکردی، مستقل از سایر سنجه‌ها است.

۱۱-۲

شایستگی

توانایی به‌کارگیری دانش ومهارت‌ها جهت رسیدن به نتایج موردنظر است.

۱۲-۲

محرمانگی

خصوصیتی که اطلاعات برای افراد، هستارها یا فرآیندهای (۲-۶۱) غیرمجازدر دسترس نبوده یا افشا نشود.

۱۳-۲

انطباق

تحقق یک الزام (۲-۶۳) است.

یادآوری ۱-اصطلاح«متابعت[1]» مترادف است ولی مناسب نیست[2].

۱۴-۲

پیامد

خروجی یک رویداد (۲-۲۵) که بر اهداف (۲-۵۶) تأثیر می‌گذارد.

[منبع:ISO Guide73:2009]

یادآوری ۱-رویدادی که ممکن است منجر به طیفی از پیامدها شود.

یادآوری ۲-پیامدی که ممکن است قطعی یا غیرقطعی باشد و معمولاً در زمینهٔ امنیت اطلاعات، منفی است.

یادآوری ۳-پیامدهایی که می‌تواند کمّی یا کیفی بیان شوند.

یادآوری ۴-پیامدهای اولیه می‌توانند به‌واسطه اثرگذاری تأثیرات آن، تشدید و گسترش یابند.

۱۵-۲

بهبود مستمر

فعالیتی بازگشتی جهت بهسازی عملکرد (۲-۵۹) است.

1- Conformance

۲- در متن انگلیسی این متن آمده است ولی در متن فارسی می توان این دو عبارت را به جای یکدیگر استفاده کرد.

۱۶-۲

کنترل

اقدامی که مخاطره (۲-۶۸) را اصلاح می‌کند.

[منبع:ISO Guide73:2009]

یادآوری ۱-کنترل‌ها می‌توانند شامل هر فرآیند، خط‌مشی، افزاره، روش یا هر اقدام دیگری شود که مخاطره را اصلاح کند.

یادآوری ۲-کنترل‌ها ممکن است همیشه منجر به اثر اصلاحی مفروض و موردنظر نشود.

۱۷-۲

هدف کنترلی

بیانیه‌ای که آنچه باید در نتیجهٔ پیاده‌سازی کنترل‌ها (۲-۱۶) به دست آید را توصیف می‌کند.

۱۸-۲

اصلاح

اقدامی که برای از بین بردن عدم انطباق (۲-۵۳) شناسایی‌شده انجام می‌گیرد.

۱۹-۲

اقدام اصلاحی

اقدامی که برای از بین بردن علت عدم انطباق (۲-۵۳) و جلوگیری از تکرار آن انجام می‌شود.

۲۰-۲

داده

مجموعه‌ای از مقادیر که به سنجه‌های مبنا (۲-۱۰)، سنجه‌های مشتق (۲-۲۲) و/یا نشانگرها (۲-۳۰) نسبت داده‌شده است.

[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵:سال ۱۳۸۷]

یادآوری ۱-این تعریف فقط در زمینهٔ ISO/IEC27004:2009 تعریف می‌شود.

۲۱-۲

معیار تصمیم‌گیری

آستانه‌ها، اهداف یا الگوهایی که با به‌کارگیری آن‌ها، نیاز به اقدام یا بررسی بیشتر تعیین می‌شود، یا سطح اطمینان در نتایج ارائه‌شده توصیف می‌شود.

[منبع:استاندارد ملی ایران شماره ۱۲۷۵۵:سال ۱۳۸۷]

۲۲-۲

سنجه مشتق

سنجه‌ای (۲-۴۷) است که به‌صورت تابعی از مقادیر دو یا چند سنجهٔ مبنا (۲-۱۰) تعریف‌شده است.
[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵:سال ۱۳۸۷]

۲۳-۲

اطلاعات مستند

اطلاعاتی که سازمان (۲-۵۷) ملزم به کنترل و نگهداری آن‌ها است و همچنین رسانه‌ای که اطلاعات روی آن نگهداری می‌شود.

یادآوری ۱- اطلاعات مستند می‌تواند در هر قالب و روی هر رسانه‌ای بوده و از هر منبعی تأمین‌شده باشد.

یادآوری ۲-اطلاعات مستند می‌تواند اشاره داشته باشد به:

- سیستم مدیریت (۲-۴۶)، شامل فرآیندهای (۲-۶۱) مرتبط؛
- اطلاعات ایجادشده جهت عملیات سازمان (مستندسازی)؛
- شواهد نتایج به‌دست‌آمده (سوابق).

۲۴-۲

اثربخشی

میزانی که فعالیت‌های طرح‌ریزی‌شده تحقق‌یافته و نتایج طرح‌ریزی‌شده به‌دست‌آمده است.

۲۵-۲

رویداد

وقوع یا تغییر مجموعه‌ای ویژه از شرایط است.

[منبع: ISO Guide73:2009]

یادآوری ۱-رویداد[1] می‌تواند یک یا چندین اتفاق[2] بوده و می‌تواند چندین علت داشته باشد.

یادآوری ۲-رویداد می‌تواند شامل مواردی باشد که اتفاق نیفتاده است.

یادآوری ۳-به رویداد ممکن است «رخداد[3]» یا «حادثه[4]» هم گفته شود.

1- Event
2- Occurrence
3- Incident
4 - Accident

۲۶-۲

مدیریت اجرایی

فرد یا گروهی از افراد که از طرف هیأت حاکم[1] (۲-۲۹) برای پیاده‌سازی راهبردها و خط‌مشی‌ها جهت تحقق اهداف سازمان (۲-۵۷) دارای اختیار هستند.

یادآوری ۱-مدیریت اجرایی گاهی مدیریت ارشد نامیده می‌شود و می‌تواند دربرگیرندهٔ مسئول ارشد اجرایی، مسئول ارشد مالی، مسئول ارشد اطلاعات و نقش‌های مشابه باشد.

۲۷-۲

زمینهٔ بیرونی

محیط بیرونی که سازمان در آن به دنبال دستیابی به اهداف خود است.

[منبع: ISO Guide73:2009]

یادآوری ۱-زمینهٔ بیرونی می‌تواند شامل موارد زیر باشد:

- محیط فرهنگی، اجتماعی، سیاسی، قانونی[2]، مقررات تنظیمی[3]، فناورانه، اقتصادی، طبیعی، رقابتی، به‌صورت بین-المللی، ملی، منطقه‌ای یا محلی؛
- پیشران‌ها و روندهای کلیدی تأثیرگذار بر اهداف (۲-۵۶) سازمان (۲-۵۷)؛ و
- ارتباطات، ادراکات[4] و ارزش‌های ذی‌نفعان (۲-۸۲) بیرونی؛

۲۸-۲

حاکمیت امنیت اطلاعات

سیستمی است که بر اساس آن فعالیت‌های امنیت اطلاعات سازمان (۲-۵۷) هدایت و کنترل می‌شود.

۲۹-۲

هیأت حاکم

فرد یا گروهی از افراد که پاسخگوی انطباق و عملکرد (۲-۵۹) سازمان(۲-۵۷) هستند.

یادآوری ۱-هیأت حاکم در برخی حوزه‌ها، می‌تواند هیأت مدیره باشد.

1- Governing body
2- Legal
3- Regulatory
4- Perceptions

۳۰-۲

نشانگر

سنجه‌ای (۲-۴۷) است جهت تخمین یا ارزشیابی صفات (۲-۴) مشخص که با توجه به نیازهای اطلاعاتی (۲-۳۱) تعریف‌شده از مدل تحلیلی (۲-۲) مشتق شده است.

۳۱-۲

نیاز اطلاعاتی

بینش لازم جهت مدیریت اهداف، مقاصد، مخاطرات و مشکلات است.

[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵: سال ۱۳۸۷]

۳۲-۲

تسهیلات پردازش اطلاعات

هر سیستم، خدمت یا زیرساخت پردازش اطلاعات، یا مکان فیزیکی میزبان آن است.

۳۳-۲

امنیت اطلاعات

حفظ محرمانگی (۲-۱۲)، یکپارچگی(۲-۴۰) و دسترس‌پذیری (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.

۳۴-۲

تداوم امنیت اطلاعات

فرآیندها (۲-۶۱) و روش‌های اجرایی جهت اطمینان از تداوم عملیات امنیت اطلاعات (۲-۳۳) است.

۳۵-۲

رویداد امنیت اطلاعات

وقوع یک حالت شناخته‌شده از سیستم، خدمت یا وضعیت شبکه که یک نقض احتمالی از خط‌مشی امنیت اطلاعات یا شکست در کنترل‌ها، یا شرایط از قبل ناشناخته که می‌تواند مرتبط با امنیت باشد را نشان می‌دهد.

۳۶-۲

رخداد امنیت اطلاعات

یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات (۲-۳۵) ناخواسته یا پیش‌بینی‌نشده که به‌احتمال‌زیاد عملیات کسب‌وکار را به خطر می‌اندازد و امنیت اطلاعات (۲-۳۳) را تهدید می‌کند.

۳۷-۲

مدیریت رخداد امنیت اطلاعات

فرآیندهایی (۲-۶۱) به‌منظور آشکارسازی، گزارش دهی، ارزیابی، پاسخ‌دهی بـه، رسـیدگی بـه و یـادگیری از رخدادهای امنیت اطلاعات (۲-۳۶) است.

۳۸-۲

جامعه اشتراک‌گذار اطلاعات

گروهی از سازمان‌ها که جهت اشتراک اطلاعات توافق دارند.

یادآوری ۱-سازمان می‌تواند یک شخص باشد.

۳۹-۲

سیستم اطلاعاتی

برنامه‌های کاربردی، خدمات، دارایی‌های فناوری اطلاعات یا سایر مؤلفه‌های اداره‌کننده[1] اطلاعات است.

۴۰-۲

یکپارچگی

خصوصیت صحت و تمامیت دارایی‌ها است.

۴۱-۲

طرف‌های علاقه‌مند

فرد یا سازمان (۲-۵۷) که می‌تواند بر فعالیت یا تصمیم اثر گذاشته، متأثر از آن شده یـا خـود را متـأثر از آن بداند.

۴۲-۲

زمینهٔ درونی

محیط درونی که سازمان در آن به دنبال دستیابی به اهداف خود است.

[منبع:ISO Guide73:2009]

یادآوری ۱-زمینه درونی می‌تواند شامل موارد زیر باشد:

- حاکمیت، ساختار سازمانی، نقش‌ها و پاسخ‌گویی‌ها؛
- خط‌مشی‌ها، اهداف و راهبردهایی که جهت دستیابی به آن‌ها وجود دارد؛

1- Handling

- ظرفیت‌ها که به‌صورت منابع و دانش (به‌عنوان‌مثال: سرمایه، زمان، افراد، فرآیندها، سیستم‌ها، فناوری‌ها) درک شده است؛
- سامانه‌های اطلاعاتی، جریان‌های اطلاعاتی و فرآیندهای تصمیم‌سازی (به‌صورت رسمی و غیررسمی)؛
- ارتباطات، ادراکات و ارزش‌های ذی‌نفعان درونی؛
- فرهنگ سازمانی؛
- استانداردها، راهنماها و مدل‌های انطباق یافته توسط سازمان؛
- شکل و گستره روابط قراردادی.

۴۳-۲

پروژه ISMS

فعالیت‌های ساختارمندکه سازمان (۲-۵۷) جهت پیاده‌سازی ISMS انجام می‌دهد.

۴۴-۲

سطح مخاطره

شدت مخاطره (۲-۶۸) که به‌صورت ترکیبی از پیامدها (۲-۱۴) و فرصت وقوع[1] (۲-۴۵) پیامدها بیان می‌شود.
[منبع:ISO Guide73:2009 ، تغییر یافته - «یا ترکیبی از مخاطرات» حذف شده است]

۴۵-۲

فرصت وقوع

شانس رویدادن چیزی است.
[منبع:ISO Guide73:2009]

۴۶-۲

سیستم مدیریت

مجموعه‌ای از عناصر مرتبط یا متعامل سازمان (۲-۵۷) جهت استقرار خط‌مشی‌ها (۲-۶۰)، اهـداف (۲-۵۶) و فرآیندها (۲-۶۱) به‌منظور دستیابی به اهداف سازمان است.

یادآوری ۱-سیستم مدیریت می‌تواند به یک یا چندین نظام مدیریتی[2] اشاره کند.

یادآوری ۲- عناصر سیستم شامل ساختار سازمانی، نقش‌ها، مسئولیت‌ها، برنامه‌ریزی، عملیات و غیره است.

یادآوری ۳-محدوده کاربرد سیستم مدیریت ممکن است شامل کل سازمان، کارکردهای مشخص و تعیین‌شده سازمان، بخش-های مشخص و تعیین‌شده سازمان یا یک یا چندین کارکرد بین، گروهی از سازمان‌ها باشد.

---

1 -likelihood

2- Discipline

۴۷-۲

سنجه

متغیری که به‌واسطهٔ نتیجهٔ سنجش (۲-۴۸) مقداری به آن نسبت داده‌شده است.

[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵:سال ۱۳۸۷]

یادآوری ۱- اصطلاح «سنجه‌ها» درمجموع برای اشاره به سنجه‌های مبنا، سنجه‌های مشتق و نشانگرها به کار می‌رود.

۴۸-۲

سنجش

فرآیند (۲-۶۱) تعیین ارزش است.

یادآوری ۱-درزمینهٔ امنیت اطلاعات (۲-۳۳)، فرآیند تعیین مقدار نیازمند اطلاعاتی در مورد اثربخشی (۲-۲۴) سیستم مدیریت امنیت اطلاعات (۲-۴۶) و کنترل‌های (۲-۱۶) مرتبط به آن است که به کمک روش سنجش (۲-۵۰)، تابع سنجش (۲-۴۹)، مدل تحلیلی (۲-۲) و معیار تصمیم‌گیری (۲-۲۱) به دست می‌آید.

۴۹-۲

تابع سنجش

الگوریتم یا محاسباتی است که برای ترکیب یک یا چندسنجهٔ مبنا (۲-۱۰) انجام می‌شود.

[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵: سال ۱۳۸۷]

۵۰-۲

روش سنجش

ترتیب منطقی کارها که به‌صورت عام تعریف‌شده است و برای کمّی کردن صفت (۲-۴) برحسب مقیاس (۲-۸۰) مشخص به کار می‌رود.

[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵: سال ۱۳۸۷]

یادآوری ۱-نوع روش سنجش وابسته به ماهیت اعمالی است که جهت کمّی سازی یک صفت مورداستفاده قرارگرفته است. دو نوع روش قابل‌تمایز است:

- ذهنی: کمّی سازی که در آن قضاوت انسان نقش دارد.
- عینی: کمّی سازی که بر اساس قواعد عددی است.

۵۱-۲

نتایج سنجش

یک یا چند نشانگر (۲-۳۰) و تفسیرهای مرتبط به آن‌ها که به نیاز اطلاعاتی (۲-۳۱) اشاره می‌کند.

۵۲-۲

پایش

تعیین وضعیت سیستم، فرآیند (۲-۶۱) یا فعالیت است.

یادآوری ۱-برای تعیین وضعیت ممکن است نیاز به بررسی، نظارت یا مشاهده انتقادی باشد.

۵۳-۲

عدم انطباق

برآورده نشدن یک الزام (۲-۶۳) است.

۵۴-۲

سلب انکار

توانایی اثبات وقوع رویداد یا اقدام ادعا شده و هستارهای منشأ آن است.

۵۵-۲

شیء

عنصری که به‌واسطهٔ سنجش (۲-۴۸) صفت‌هایش (۲-۴) مشخص‌شده است.

۵۶-۲

هدف

نتیجه‌ای که باید به دست آید.

یادآوری ۱-هدف می‌تواند راهبردی، راه‌کنشی[1] یا عملیاتی باشد.

یادآوری ۲-اهداف می‌تواند به نظام‌های مختلف مرتبط باشد (مانند اهداف مالی، سلامت و امنیتی و محیطی) و در سطوح مختلف به کار گرفته شود (مانند سطح راهبردی، گستره سازمان، پروژه، محصول و فرآیند (۲-۶۱)).

یادآوری ۳-هدف می‌تواند به اشکال دیگری مانند دستاورد موردنظر، هدف، معیارعملکردی، هدف امنیت اطلاعات یا با استفاده از کلماتی با معانی مشابه (مانند منظور، نتیجه، مقصود) بیان شود.

یادآوری ۴ –درزمینهٔ سیستم‌های مدیریت امنیت اطلاعات، اهداف امنیت اطلاعات توسط سازمان تعیین‌شده و با خط‌مشی امنیت اطلاعات سازگار می‌شوند تا نتایج موردنظر به دست آید.

[1] tactical

۵۷-۲

سازمان

فرد یا گروهی از افراد که وظایف خود را با مسئولیت‌ها، اختیارات و روابط بر عهده‌دارند تا بـه اهدافشـان (۲-۵۶) دست یابند.

یادآوری ۱-مفهوم سازمان، کسب‌وکار فردی، شرکت تجاری، شرکت سهامی، موسسه بازرگانی، تشکیلات اقتصـادی، نماینـدگی مجاز، مشارکت، خیریه و مؤسسات، یا قسمتی یا ترکیبی از اینها، خواه با هم همکاری کنند یا خیر، خصوصی باشند یـا عمـومی باشند را شامل می شود اما محدود به اینها نیست.

۵۸-۲

برون‌سپاری کردن

ترتیب دادن امور به‌گونه‌ای که یک سازمان (۲-۵۷) بیرونی، بخشی از وظایف یا فرآیندهای (۲-۶۱) سازمان را انجام دهد.

یادآوری ۱- سازمان بیرونی خارج از قلمرو کاربرد سیستم مدیریتی (۲-۴۶) است، هرچند وظایف یا فرآیند برون‌سـپاری شـده، درون محدوده باشد.

۵۹-۲

عملکرد

نتیجهٔ قابل‌اندازه‌گیری است.

یادآوری ۱-عملکرد می‌تواند به یافته‌های کیفی یا کمّی مرتبط باشد.

یادآوری ۲ -عملکرد می‌تواند مرتبط به مدیریت فعالیت‌ها، فرآیندها (۲-۶۱)، محصولات (شامل خدمات) سیستم‌ها یا سازمان-ها (۲-۵۷) شود.

۶۰-۲

خط‌مشی

خواسته‌ها و جهت‌گیری سازمان (۲-۵۷) که توسط مدیریت ارشد (۲-۸۴) به‌صورت رسمی بیان‌شده است.

۶۱-۲

فرآیند

مجموعه‌ای از فعالیت‌های مرتبط و متعامل که ورودی‌ها[1] رابه خروجی‌ها[2] تبدیل می‌کند.

1- Inputs
2- Outputs

۶۲-۲

اطمینان پذیری

خصوصیت ثبات و پایداری در رفتار و نتایج موردنظر است.

۶۳-۲

الزام

نیاز یا انتظاری که تصریح‌شده، به‌صورت عام دلالت ضمنی دارد، یا دارای اجبار قانونی است.

یادآوری ۱-«به‌صورت عام دلالت ضمنی داشته» به این معنی است که آن نیاز یا انتظار مورد نظر به‌صورت ضمنی، اقدامی متداول و مرسوم برای سازمان و طرف‌های علاقه‌مند محسوب می‌شود.

یادآوری ۲-الزام مشخص‌شده، الزامی است که تصریح‌شده است به‌عنوان‌مثال در اطلاعات مستند.

۶۴-۲

مخاطره باقیمانده

مخاطره (۲-۶۸) باقیمانده، پس از برطرف‌سازی مخاطره (۲-۷۹) است.

یادآوری ۱ -مخاطره باقیمانده می‌تواند شامل مخاطره شناسایی نشده باشد.

یادآوری ۲ -مخاطره باقیمانده تحت عنوان«مخاطرات نگه‌داشته شده[1]» نیز شناخته می‌شود.

۶۵-۲

بازنگری

فعالیتی است که جهت تعیین میزان تناسب، کفایت و اثربخشی (۲-۲۴) یک موضوع به‌منظور دستیابی به اهداف مقررشده انجام می‌شود.

[منبع: ISO Guide73:2009]

۶۶-۲

شیء مورد بازنگری

عنصر[2] مشخصی که مورد بازنگری قرار می‌گیرد.

۶۷-۲

هدف بازنگری

بیانه‌ای که آنچه باید ازنتیجه بازنگری به دست آید را توصیف می‌کند.

1- Retained risk
2- Item

۶۸-۲

مخاطره

اثر عدم قطعیت[1] بر اهداف است.

[منبع: ISO Guide73:2009]

یادآوری ۱ -اثر، انحراف از انتظار است، که می تواند مثبت یا منفی باشد .

یادآوری ۲ -عدم قطعیت، وضعیتی از کمبود (هرچند جزئی) اطلاعات مرتبط، یا نقص در درک و دانش مربوط بـه رویـداد (۲-۲۵) یا پیامدها (۲-۱۴) یا فرصت وقوع (۲-۴۵) است.

یادآوری ۳-مخاطره معمولاً با ارجاع به رویدادهای (۲-۲۵) بالقوه و پیامدها (۲-۱۴) یا ترکیبی از آن‌ها مشخص می‌شود.

یادآوری ۴-مخاطره معمولاً به‌صورت ترکیبی از پیامدهای (۲-۱۴) یک رویداد (شامل تغییر شـرایط) و فرصـت وقـوع (۲-۴۵) مرتبط با آن بیان می‌شود.

یادآوری ۵-در زمینهٔ سیستم‌های مدیریت امنیت اطلاعات، مخاطرات امنیت اطلاعات می‌تواند به‌صورت تأثیر عدم قطعیـت بـر اهداف امنیت اطلاعات بیان شود.

یادآوری ۶ -مخاطرهٔ امنیت اطلاعات با پتانسـیل بهـره‌جـویی تهدیـدات (۲-۸۳) از آسـیب‌پـذیری‌هـای (۲-۸۹) یـک دارایـی اطلاعاتی یا گروهی از آن‌ها و آسیب‌رسانی از طریق آن به سازمان، مرتبط است.

۶۹-۲

پذیرش مخاطره

تصمیم آگاهانه جهت به عهده گرفتن یک مخاطره (۲-۶۸) خاص است.

[منبع:ISO Guide73:2009]

یادآوری ۱-پذیرش مخاطره می‌تواند بدون برطرف‌سازی (۲-۷۹) مخاطره یا طی فرآیند برطرف‌سازی مخاطره انجام شود.

یادآوری ۲-مخاطرات پذیرفته‌شده مورد پایش (۲-۵۲) و بازنگری (۲-۶۵) قرار می‌گیرند.

۷۰-۲

تحلیل مخاطره

فرآیند درک ماهیت مخاطره (۲-۶۸) و تعیین سطح مخاطره (۲-۴۴) است.

[منبع:ISO Guide73:2009]

یادآوری ۱-تحلیل مخاطره مبنایی برای ارزشیابی مخاطره (۲-۷۴) و تصمیمات مرتبط با برطرف‌سازی مخاطره (۲-۷۹) فـراهم می‌کند.

یادآوری ۲-تحلیل مخاطره شامل تخمین مخاطره است.

1- Uncertainty

۷۱-۲

ارزیابی مخاطره

فرآیند (۲-۶۱) کلان شناسایی (۲-۷۵)، تحلیل (۲-۷۰) و ارزشیابی مخاطره (۲-۷۴) است.

[منبع:ISO Guide73:2009]

۷۲-۲

اطلاع‌رسانی و مشاوره مخاطره

فرآیندهای پیوسته و تکرارپذیر است که سازمان جهت تهیه، به اشتراک‌گذاری و کسب اطلاعات و همچنین مذاکره با ذی‌نفعان(۲-۸۲) در ارتباط با مدیریت مخاطره (۲-۶۸) انجام می‌دهد.

یادآوری ۱ –اطلاعات ممکن است به وجود، ماهیت، شکل، فرصت وقوع، اهمیت، ارزشیابی، قابل‌پذیرش بودن یا برطرف‌سازی مخاطره، مرتبط باشد.

یادآوری ۲ –مشاوره یک فرآیند دوطرفه جهت ارتباط آگاهانه بین سازمان و ذی‌نفعان سازمان است که در مورد یک موضوع و قبل از اخذ تصمیم یا جهت‌گیری در مورد آن صورت می‌گیرد. مشاوره:

- فرآیندی است که به‌واسطه توانمندی و نه به‌واسطه قدرت، بر تصمیم اثر می‌گذارد؛
- ورودی جهت تصمیم‌سازی مشارکتی به حساب نمی آید.

۷۳-۲

معیار مخاطره

عبارات مرجعی که اهمیت مخاطره (۲-۶۸) به نسبت آن‌ها ارزشیابی می‌شود.

[منبع: ISO Guide73:2009]

یادآوری ۱ –معیار مخاطره بر مبنای اهداف سازمانی و همچنین زمینه درونی و بیرونی سازمان است.

یادآوری ۲ –معیار مخاطره ممکن است از استانداردها، قوانین، خط‌مشی‌ها و سایر الزامات استخراج شود.

۷۴-۲

ارزشیابی مخاطره

فرآیند (۲-۶۱) مقایسه نتایج تحلیل مخاطره (۲-۷۰) با معیارهای مخاطره (۲-۷۳) جهت تعیین اینکه آیا مخاطره (۲-۶۸) و/یا شدت آن قابل‌پذیرش یا قابل‌تحمل است.

[منبع: ISO Guide73:2009]

یادآوری ۱–ارزشیابی مخاطره به تصمیم‌گیری درموردبرطرف‌سازی مخاطره (۲-۷۹) کمک می‌کند.

۷۵-۲

شناسایی مخاطره

فرآیند یافتن، تشخیص و توصیف مخاطرات (۲-۶۸) است.

[منبع:ISO Guide73:2009]

یادآوری ۱-شناسایی مخاطره شامل شناسایی منابع مخاطره، رویدادها، علل آن‌ها و پیامدهای بالقوه رویدادها است.

یادآوری ۲ -شناسایی مخاطره می‌تواند داده‌های تاریخچه‌ای، تحلیل‌های نظری، اظهارنظرهای آگاهانه و کارشناسی و نیازهای ذی‌نفعان را به کارگیرد.

۷۶-۲

مدیریت مخاطره

فعالیت‌های هماهنگ جهت هدایت و کنترل سازمان (۲-۵۷) با توجه به مخاطره (۲-۶۸) است.

[منبع: ISO Guide73:2009]

۷۷-۲

فرآیند مدیریت مخاطره

به‌کارگیری نظام‌مند خط‌مشی‌ها، روش‌های اجرایی و اقدامات مدیریتی در فعالیت‌های برقراری ارتباط، مشاوره، استقرار زمینه و همچنین شناسایی، تحلیل، ارزشیابی، برطرف‌سازی، پایش و بازنگری مخاطره (۲-۶۸) است.

[منبع: ISO Guide73:2009]

یادآوری ۱-ISO/IEC27005 اصطلاح «فرآیند» را جهت توصیف کلّی مدیریت مخاطره به کار می‌برد. عناصر درون فرآیند مدیریت مخاطره اصطلاحاً «فعالیت» نامیده می‌شود.

۷۸-۲

مالک مخاطره

فرد یا هستاری جهت مدیریت مخاطره (۲-۶۸) که صاحب‌اختیار و پاسخ‌گو است.

[منبع: ISO Guide73:2009]

۷۹-۲

برطرف سازی مخاطره

فرآیند (۲-۶۱) تعدیل مخاطره (۲-۶۸) است.

[منبع: ISO Guide73:2009]

یادآوری ۱-برطرف‌سازی مخاطره می‌تواند شامل موارد زیر باشد:

- اجتناب از مخاطره با تصمیم‌گیری در مورد عدم شروع یا ادامه فعالیتی که مخاطره را افزایش می‌دهد؛
- پذیرش یا افزایش مخاطره به‌منظورفرصت‌سازی؛
- حذف منبع مخاطره؛
- تغییر فرصت وقوع؛

- تغییر پیامدها؛
- اشتراک‌گذاری مخاطره با بخش یا بخش‌های دیگر (شامل قراردادها و تأمین مالی مخاطره)؛ و
- حفظ مخاطره با انتخاب آگاهانه؛

یادآوری ۲-برطرف‌سازی‌های مخاطره که در جهت رسیدگی به پیامدهای منفی انجام می‌شود، «کاهش مخاطره»، «حذف مخاطره»، «اجتناب مخاطره»، «تقلیل مخاطره» نیز نامیده می‌شود.

یادآوری ۳-برطرف سازی مخاطره می تواند منجر به ایجاد مخاطرات جدید یا تغییر مخاطرات موجود شود.

۸۰-۲

مقیاس

مجموعهٔ مرتب از مقادیر به‌صورت پیوسته یا گسسته یا مجموعه‌ای از رده‌بندی‌ها که یک صفت (۲-۴) به آن نگاشت شده است.

[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵: سال ۱۳۸۷]

یادآوری ۱ – نوع مقیاس وابسته به ماهیت روابط بین مقادیر مبتنی بر آن مقیاس است. چهار نوع مقیاس معمولاً تعریف می‌شود:

- اسمی: مقادیر سنجش رده‌بندی‌شده هستند؛
- ترتیبی: مقادیر سنجش دارای رتبه‌بندی هستند؛
- بازه‌ای: مقادیر سنجش دارای فواصل مساوی مطابق با کمیت‌های یکسان صفت هستند؛
- نسبتی: مقادیر سنجش دارای فواصل مساوی مطابق با کمیت‌های یکسان صفت هستند، درجایی که مقدار صفر مطابق با نبود صفت است.

موارد فوق صرفاً مثال‌هایی از انواع مقیاس‌ها است.

۸۱-۲

استاندارد پیاده‌سازی امنیت

مستندی که روش‌های مجاز جهت تحقق امنیت را مشخص می‌کند.

۸۲-۲

ذینفع

فرد یا سازمانی که می‌تواند بر تصمیم یا فعالیت اثر بگذارد، یا اثر بگیرد یا خود را متأثر از آن بداند.

[منبع: ISO Guide73:2009]

۸۳-۲

تهدید

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

۸۴-۲

مدیریت ارشد

فرد یا گروهی از افراد که هدایت و کنترل سازمان (۲-۵۷) را در بالاترین سطح به عهده‌دارند.

یادآوری ۱-مدیریت ارشد قدرت تفویض اختیار و فراهم‌سازی منابع درون سازمان را در اختیار دارد.

یادآوری ۲- اگر قلمرو کاربرد سیستم مدیریت (۲-۴۶) فقط بخشی از سازمان (۲-۵۷) را پوشش دهد، در این صورت مدیریت ارشد اشاره به افرادی دارد که آن بخش سازمان (۲-۵۷) را هدایت و کنترل می‌کنند.

۸۵-۲

هستار قابل‌اعتماد تبادل اطلاعات

سازمان مستقلی که مبادله اطلاعات درجامعه اشتراک‌گذاران اطلاعات را حمایت می‌کند.

۸۶-۲

واحد سنجش

کمیّتی مشخص که طبق توافقی تعریف و پذیرفته‌شده است و به کمک آن کمیّت، اندازه سایر کمیّت‌های هم نوع نسبت به آن با یکدیگر مقایسه می‌شوند.
[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵: سال ۱۳۸۷]

۸۷-۲

اعتبارسنجی

تائیدی است بر اساس تهیه شواهد عینی، مبنی بر اینکه الزامات مطابق با کاربرد یا استفاده خاص و تعیین-شده برآورده شده است.
[منبع: : استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

۸۸-۲

درستی‌سنجی

تائیدی است بر اساس تهیه شواهد عینی، مبنی بر اینکه الزامات مشخص‌شده برآورده شده است.
[منبع: : استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

یادآوری ۱- همچنین می‌تواند آزمون انطباق نامیده شود.

۸۹-۲

آسیب‌پذیری

ضعف یک دارایی یا کنترل (۲-۱۶) که ممکن است توسط یک یا چندین تهدید (۲-۸۳) موردسوء استفاده قرار گیرد.

۳ سیستم‌های مدیریت امنیت اطلاعات

۳-۱ مقدمه

سازمان‌ها از هر نوع و اندازه:

الف- اطلاعات را جمع‌آوری، پردازش، ذخیره و ارسال می‌کنند؛

ب- تشخیص می‌دهند که اطلاعات و فرآیندها، سیستم‌ها، 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، مواردی را که می‌دانند در معرض مخاطره قرار دارند موردتوجه قرار می‌دهند.

تمام اطلاعات نگهداری و پردازش‌شده توسط سازمان، در معرض تهدیدهای حمله، خطا، عوامل طبیعی (مانند سیل یا آتش‌سوزی) و مانند آن قرار دارند و با آسیب‌پذیری‌های ذاتی در کاربرد آن‌ها مواجه هستند. اصطلاح امنیت اطلاعات عموماً 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، موردحفاظت مناسب قرار گیرند. دسترسی به‌موقع به اطلاعات دقیق و کامل از سوی افرادی با نیاز مجازشده، باعث تقویت بازدهی کسب‌وکار می‌شود.

حفاظت از دارایی‌های اطلاعاتی از طریق تعریف، به دست آوردن، نگهداری و بهبود مؤثر امنیت اطلاعات، برای توانمندسازی سازمان به‌منظور 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 غیرقابل‌قبول را برطرف می‌کنند، عموماً اجزای مدیریت امنیت اطلاعات قلمداد می‌شوند.

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

الف- اثربخشی کنترل‌ها و روش‌های اجرایی پیاده‌سازی شده را پایش و ارزشیابی کنند؛

ب- مخاطرات نوظهوری را که باید برطرف شوند، شناسایی کنند؛ و

پ- کنترل‌های مناسب را برحسب نیاز برگزینند، پیاده‌سازی کنند و بهبود دهند.

به‌منظور مرتبط و هماهنگ نمودن این‌گونه فعالیت‌های امنیت اطلاعات، هر سازمان باید خط‌مشی و اهداف خود برای امنیت اطلاعات را تعیین کند و با استفاده از سیستم مدیریت به‌طورمؤثری آن اهداف را به دست آورد.

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

۱-۲-۳ مرورکلی و اصول

سیستم مدیریت امنیت اطلاعات (ISMS) شامل خط‌مشی‌ها، روش‌های اجرایی، راهنمایی‌ها و فعالیت‌ها و منابع مرتبط است که توسط سازمان در تلاش برای محافظت از دارایی‌های اطلاعاتی خود به‌صورت تجمیعی مدیریت می‌شود. سیستم مدیریت امنیت اطلاعات یک رویکرد نظام‌مند برای استقرار، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات یک سازمان به‌منظور تحقق اهداف کسب‌وکار فراهم می‌سازد که مبتنی بر ارزیابی مخاطره و سطوح قابل‌قبول مخاطره سازمان برای برطرف‌سازی و مدیریت مؤثر مخاطرات طراحی‌شده است. تحلیل الزامات به‌منظور حفاظت از دارایی‌های اطلاعاتی و اعمال کنترل‌های مناسب، برای اطمینان از حفاظت لازم از این دارایی‌های اطلاعاتی در صورت نیاز، به پیاده‌سازی موفقیت‌آمیز ISMS کمک می‌کند. اصول بنیادی زیر نیز به پیاده‌سازی موفقیت‌آمیز ISMS کمک می‌کنند:

الف- آگاهی نسبت به‌ضرورت امنیت اطلاعات؛

ب- تخصیص مسئولیت برای امنیت اطلاعات؛

پ- تلفیق تعهد مدیریت با منافع ذی‌نفعان؛

ت- تقویت ارزش‌های اجتماعی؛

ث- ارزیابی مخاطرات جهت اعمال کنترل‌های مناسب برای رسیدن به سطوح قابل‌قبول مخاطره؛

ج- در نظر گرفتن امنیت به‌عنوان عنصر ضروری سیستم‌ها و شبکه‌های اطلاعاتی؛

چ- پیشگیری و تشخیص فعال رخدادهای امنیت اطلاعات؛

ح- اطمینان از رویکردی جامع برای مدیریت امنیت اطلاعات؛ و

خ- تداوم ارزیابی مجدد امنیت اطلاعات و اعمال اصلاحات در صورت صلاحدید.

۲-۲-۳ اطلاعات

اطلاعات، دارایی است که همانند سایر دارایی‌های مهم کسب‌وکار برای فعالیت سازمان ضروری است و درنتیجه نیاز به حفاظت مناسب دارد. اطلاعات را می‌توان به شکل‌های بسیاری ذخیره کرد، ازجمله: به شکل دیجیتالی (برای مثال داده‌های ذخیره‌شده دررسانه 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 به‌صورت شفاهی انتقال داد. اطلاعات، به هر شکلی که باشد، یا با هر روشی که انتقال یابد، همیشه به حفاظت مناسب نیاز دارد.

در بسیاری از سازمان‌ها، اطلاعات به فناوری ارتباطات و اطلاعات وابسته است. این فناوری عنصری اساسی در سازمان است و ایجاد، پردازش، ذخیره‌سازی، انتقال، حفاظت و از بین بردن اطلاعات را تسهیل می‌کند.

۳-۲-۳ امنیت اطلاعات

امنیت اطلاعات دارای سه بعد اصلی است که عبارتند از محرمانگی، دسترس‌پذیری و یکپارچگی. امنیت اطلاعات شامل به‌کارگیری و مدیریت معیارهای امنیتی مناسبی است که بازه گسترده‌ای از تهدیدات را موردتوجه قرار می‌دهد و به دنبال اطمینان از موفقیت پایدار و تداوم کسب‌وکار و در جهت کمینه کردن اثرات رخدادهای امنیت اطلاعات است.

امنیت اطلاعات با پیاده‌سازی مجموعه‌ای از کنترل‌های کاربردپذیر به دست می‌آید که از طریق فرآیند مدیریت مخاطره، انتخاب‌شده و با استفاده از ISMS مدیریت می‌شود که شامل خط‌مشی‌ها، فرآیندها، روش‌های اجرایی، ساختارهای سازمانی، نرم‌افزارها و سخت‌افزارها به‌منظور حفاظت از دارایی‌های اطلاعاتی شناسایی‌شده است. به‌منظور اطمینان از دستیابی به اهداف امنیت اطلاعات وکسب‌وکار سازمان، این کنترل‌ها باید تعیین، پیاده‌سازی، پایش، بازنگری و در صورت نیاز بهبود داده شوند. کنترل‌های مرتبط با امنیت اطلاعات باید به‌صورت تنگاتنگی با فرآیندهای کسب‌وکار سازمان یکپارچه‌شده باشند.

۴-۲-۳ مدیریت

مدیریت شامل فعالیت‌های هدایت، کنترل و بهبود مستمر سازمان در بستر ساختارهای مناسب است. فعالیت‌های مدیریتی شامل اقدام یا روش یا شیوه سازمان‌دهی، اداره کردن، هدایت، نظارت و کنترل منابع است. ساختارهای مدیریتی از یک فرد در سازمانی کوچک تا سلسله‌مراتب مدیریتی با افرادی بسیار در سازمان‌های بزرگ، گسترش می‌یابد.

از دیدگاهISMS، مدیریت عبارت از نظارت و تصمیم‌گیری‌های لازم برای رسیدن به اهداف کسب‌وکار از طریق حفاظت از دارایی‌های اطلاعاتی سازمان است. مدیریت امنیت اطلاعات، از طریق تدوین و استفاده از خط‌مشی‌ها، روش‌های اجرایی و راهنماهای امنیتی بیان می‌شود، سپس توسط تمام افراد دست‌اندرکار[1] سازمان در کل سازمان اعمال می‌شود.

۵-۲-۳ سیستم مدیریت

سیستم 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.

سیستم مدیریت ازلحاظ امنیت اطلاعات، سازمان را قادر می‌سازد تا:

الف- الزامات امنیت اطلاعات مشتریان و سایر ذی‌نفعان را برآورده سازد؛

ب- فعالیت‌ها وطرح‌های سازمان را بهبود دهد؛

پ- اهداف امنیت اطلاعات سازمان را محقق سازد؛

---

1 -Individual associated

ت- با مقررات، قوانین والزامات[1] صنفی تطبیق یابد؛ و

ث- دارایی‌های اطلاعاتی را به‌صورت سازمان‌یافته‌ای مدیریت کند به‌طوری‌که بهبود مستمر وسازگاری با اهداف کنونی سازمان تسهیل شود.

۳-۳ رویکرد فرآیندی[2]

سازمان‌ها باید فعالیت‌های بسیاری را تعیین و مدیریت کنند تا کارکرد مؤثر و کارآمدی داشته باشند. هر فعالیتی که از منابع استفاده می‌کند، باید مدیریت شود تا تبدیل ورودی‌ها به خروجی‌ها را با به‌کارگیری مجموعه‌ای از فعالیت‌های مرتبط و متعامل که یک فرآیند نیز نامیده می‌شود، ممکن سازد. ورودی یک فرآیند می‌تواند به‌طور مستقیم ورودی فرآیند دیگری باشد و عموماً این تبدیل در شرایط کنترل‌شده و برنامه‌ریزی‌شده صورت‌می‌گیرد. به‌کارگیری سیستمی از فرآیندها در یک سازمان، همراه با شناسایی وتعامل این فرآیندها و مدیریت آن‌ها را می‌توان «رویکردفرآیندی» نامید.

۴-۳ چرا ISMS مهم است؟

مخاطرات مرتبط با دارایی‌های اطلاعاتی سازمان باید موردتوجه قرار گیرند. رسیدن به امنیت اطلاعات به مدیریت مخاطره نیاز دارد و شامل مخاطرات ناشی از تهدیدهای فیزیکی، انسانی وفناوری مرتبط با تمام اشکال اطلاعات درون‌سازمانی و مورداستفاده سازمان می‌شوند.

انتظار می‌رود پذیرش ISMS، تصمیمی راهبردی برای سازمان باشد و لازم است این تصمیم بر طبق نیازهای سازمان، کاملاً یکپارچه، متناسب[3] و به‌روز شود.

طراحی و پیاده‌سازیISMS سازمان، تحت تأثیر نیازها و اهداف سازمان، الزامات امنیتی، فرآیندهای کسب‌و-کار به کارگرفته‌شده 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 دیگر طرف‌های سوم مرتبط منعکس شود.

در دنیای به‌هم‌پیوسته[4]، اطلاعات و فرآیندها، سیستم‌ها و شبکه‌های مرتبط، دارایی‌های حیاتی کسب‌وکار را تشکیل می‌دهند. سازمان‌ها و سیستم‌ها و شبکه‌های اطلاعاتی آن‌ها، با تهدیدهای امنیتی از سوی گستره‌ی وسیعی از منابع شامل تقلب رایانه‌ای[5]، جاسوسی[6]، خرابکاری[7]، تخریب[8]، آتش‌سوزی و سیل روبرو می‌شوند.

1 - Mandates
2 - Process Approach
3 - Scaled
4 - Interconnected World
5 - Computer assited fraud
6 - Espionage
7 - Sabotage
8 - Vandalism

آسیب زدن به سیستم‌ها و شبکه‌ها اطلاعاتی با علت کدهای مخرب، رخنه‌گری رایانه‌ای و حملات انکار خدمت (DoS)[1]، بیش از پیش فراگیر، جاه‌طلبانه‌تر و به‌طورفزاینده‌ای پیچیده شده است.

ISMS برای کسب‌وکارهای هر دو بخش عمومی و خصوصی مهم است. در هر صنعتی، ISMS، عاملی توانمندساز[2] است که از کسب‌وکار 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. به‌علاوه، توزیع افزاره‌های ذخیره‌سازی سیار که حاوی دارایی‌های اطلاعاتی است، می‌تواند اثربخشی کنترل‌های مرسوم را تضعیف کند. پذیرش استانداردهای خانواده ISMS می‌تواند نشان‌دهنده‌ی توانایی سازمان در به‌کارگیری اصول امنیت اطلاعات قابل‌درک متقابل و پایدار، برای شرکای تجاری و سایر طرف‌های علاقه‌مند باشد.

دربسیاری موارد امنیت اطلاعات در طراحی و توسعه سیستم‌های اطلاعاتی در نظر گرفته نمی‌شود. به‌علاوه، امنیت اطلاعات را اغلب راهکاری فنی تلقی می‌کنند. به‌هرحال، امنیتی که از طریق ابزارهای فنی به دست می‌آید، محدود و ممکن است بدون پشتیبانی مدیریت و روش‌های اجرایی مناسب در بستر ISMS، بی‌تأثیر باشد. گنجاندن امنیت درسیستم اطلاعاتی پس از پیاده‌سازی کامل 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 دارایی‌های اطلاعاتی، مبتنی برالزامات کسب‌وکار 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 به‌طور پیوسته در مقابل تهدیدها حفاظت می‌شود؛

ب- چارچوب ساختاریافته و فراگیری را برای شناسایی و ارزیابی مخاطرات امنیت اطلاعات، انتخاب و اعمال کنترل‌های کاربردپذیر و سنجش و بهبود اثربخشی آن‌ها در اختیار داشته باشد؛

پ- محیط کنترل خود را به‌طور مداوم بهبود دهد؛ و

ت- به‌صورت مؤثر با قوانین و مقررات تنظیم‌شده منطبق شود.

1 - Denial of Service
2 - Enabler

۳-۵ استقرار، پایش، نگهداری و بهبود ISMS

۳-۵-۱ مرور کلی

سازمان برای استقرار، پایش، نگهداری و بهبود ISMSخود، نیازمند تعهد به انجام مراحل زیر است:

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

ب- ارزیابی مخاطرات امنیت اطلاعات (طبق بند ۳-۵-۳) و برطرف سازی مخاطرات امنیت اطلاعات (طبق بند ۳-۵-۴)؛

پ- انتخاب و پیاده‌سازی کنترل‌های مرتبط برای مدیریت مخاطرات غیرقابل‌پذیرش (طبق بند ۳-۵-۴)؛ و

ت- پایش، نگهداری و بهبود اثربخشی کنترل‌های امنیتی مربوط به دارایی‌های اطلاعاتی سازمان (طبق بند ۳-۵-۶)؛

برای اطمینان از حفاظت مؤثر و مستمرISMS از دارایی‌های اطلاعاتی سازمان، لازم است مراحل «الف» تا «ت» به‌طور مداوم جهت شناسایی تغییر در مخاطرات یا در راهبردهای سازمان یا اهداف کسب‌وکار 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 شناسایی‌شده و ارزش آن‌ها؛

ب- نیازهای کسب وکار برای پردازش، ذخیره‌سازی، و تبادل اطلاعات؛ و

پ- الزامات قانونی، مقررات تنظیم‌شده وقراردادی.

ارزیابی روش‌مند مخاطرات مرتبط با دارایی‌های اطلاعاتی سازمان، شامل تحلیل تهدیدها علیه دارایی‌های اطلاعاتی، آسیب‌پذیری‌ها و فرصت وقوع تهدید در مورد دارایی‌های اطلاعاتی، و اثر بالقوه‌ی هر رخداد امنیت اطلاعات بردارایی‌های اطلاعاتی است. انتظار می‌رود هزینه کنترل‌های امنیتی مربوط متناسب با اثر قابل‌تصور از تحقق مخاطره بر کسب وکار باشد.

۳-۵-۳ ارزیابی مخاطرات امنیت اطلاعات

مدیریت مخاطرات امنیت اطلاعات به روشی مناسب برای ارزیابی و برطرف‌سازی مخاطره نیاز دارد که ممکن است شامل برآورد هزینه‌ها و منافع، الزامات قانونی، جنبه‌های اجتماعی، اقتصادی و محیطی، نگرانی‌های موردنظر ذی‌نفعان، اولویت‌ها و سایر ورودی‌ها و متغیرهای متناسب باشد.

توصیه می‌شود ارزیابی مخاطره، شناسایی، کمّی سازی و اولویت بندی مخاطره را در مقابل معیارهای پذیرش مخاطره و اهداف مرتبط با سازمان، انجام دهد. توصیه می‌شود نتایج به راهنمایی و تعیین اقدام مدیریتی

مناسب و الویت‌بندی برای مدیریت مخاطرات امنیت اطلاعات و برای پیاده سازی کنترل های برگزیده برای محافظت در برابر مخاطرات منجر شود.

توصیه می‌شود ارزیابی مخاطره شامل رویکردی نظام‌مند جهت تخمین شدت مخاطره (تحلیل مخاطره) و فرآیندی جهت مقایسه مخاطرات تخمین زده‌شده با معیارهای مخاطره داشته باشد تا میزان اهمیت مخاطرات مشخص شود (ارزشیابی مخاطره).

توصیه می‌شود ارزیابی‌های مخاطره به‌صورت دوره‌ای انجام شود تا تغییراتی را که در الزامات امنیت اطلاعات و وضعیت مخاطرات رخ می‌دهد مانند تغییر در دارایی‌ها، تهدیدات، آسیب‌پذیری‌ها، تأثیرات، ارزشیابی مخاطره و همچنین زمان بروز تغییرات مهم را منعکس کند. توصیه می‌شود ارزیابی مخاطره به شکل منظم انجام شود تا منجر به نتایج قیاس پذیر و تجدید پذیر شود.

جهت مؤثر بودن ارزیابی مخاطره امنیت اطلاعات، توصیه می‌شود ارزیابی دارای یک تعریف شفاف از محدوده کاربرد بوده و در صورت مناسب‌بودن، در ارتباط با ارزیابی‌های مخاطره در سایر حوزه‌ها باشد.

راهنمایی برای مدیریت مخاطره امنیت اطلاعات، شامل توصیه‌های ارزیابی مخاطره، برطرف‌سازی مخاطره، پذیرش مخاطره،گزارش دهی مخاطره، پایش مخاطره و بازنگری مخاطره در استاندارد ISO/IEC 27005 فراهم‌شده است. مثال‌هایی از روشگان[1] ارزیابی مخاطره نیز لحاظ شده است.

۳-۵-۴ برطرف‌سازی مخاطرات امنیت اطلاعات

توصیه می‌شود، سازمان قبل از برطرف سازی مخاطره، در مورد معیارهایی که بر اساس آن تعیین می‌کند مخاطرات قابل‌پذیرش هستند یا خیر، تصمیم‌گیری کند. مخاطرات ممکن است موردپذیرش قرار گیرند، اگر به‌عنوان‌مثال مخاطره پائین ارزیابی‌شده باشد یا اینکه هزینه برطرف‌سازی مخاطرات مقرون‌به‌صرفه نباشد. توصیه می‌شود این تصمیم‌ها، ثبت‌شده باشد.

به ازای هر یک از مخاطرات تعیین‌شده در طی ارزیابی مخاطره، نیاز است تصمیمی در ارتباط با برطرف سازی مخاطرات اتخاذ شود. انتخاب‌های ممکن جهت برطرف‌سازی مخاطره می‌تواند شامل:

الف- به‌کارگیری کنترل‌های مناسب جهت کاهش مخاطرات؛

ب- پذیرش آگاهانه و هدفمند مخاطرات مشروط بر اینکه به‌وضوح، خط‌مشی سازمان و ضوابط پذیرش مخاطرات را برآورده می‌کند؛

پ- اجتناب از مخاطره با ممانعت از تداوم فعالیت‌هایی که علت بروز مخاطرات شده است؛

ت- به اشتراک‌گذاری مخاطرات مرتبط با طرف‌های دیگر (مانند بیمه‌گذار و تأمین‌کنندگان).

1- Methodology

برای آن مخاطراتی که تصمیم برطرف سازی مخاطره، به کاربستن کنترل‌های مناسب است، توصیه می شود این کنترل‌ها انتخاب شده و پیاده‌سازی شود.

۳-۵-۵ انتخاب و پیاده‌سازی کنترل‌ها

به‌محض این‌که الزامات امنیت اطلاعات شناسایی (طبق بند ۳-۵-۲) و مخاطرات امنیت اطلاعات مربوط به دارایی‌های اطلاعاتی تعیین و ارزیابی شد (طبق بند ۳-۵-۳) و تصمیم‌گیری در مورد برطرف سازی مخاطرات امنیت اطلاعات (طبق بند ۳-۵-۴) انجام شد، آنگاه انتخاب و پیاده سازی کنترل ها برای کاهش مخاطره به کار گرفته می شود.

کنترل‌ها باید اطمینان دهند که با در نظر گرفتن موارد زیر، مخاطرات به سطح قابل پذیرش کاهش یافته‌اند:

الف- الزامات و محدودیت‌های قوانین و مقررات ملی و بین‌المللی؛

ب- اهداف سازمان؛

پ- الزامات و محدودیت‌های عملیاتی؛

ت- هزینه پیاده‌سازی و عملیاتی نمودن کنترل‌ها در ارتباط با میزان مخاطره کاهش‌یافته و مخاطرات باقیمانده به نسبت محدودیت‌ها و الزامات سازمان؛

ث- توصیه می‌شود به‌گونه‌ای پیاده‌سازی شوند تا امکان پایش، ارزشیابی و بهبود کارایی و اثربخشی کنترل-های امنیت اطلاعات در جهت حمایت از اهداف سازمان امکان‌پذیر شود. توصیه می‌شود، انتخاب و پیاده-سازی کنترل‌ها در سند بیانیه کاربردپذیری مستند شود تا به الزامات انطباق کمک کند؛

ج- باید توازنی بین سرمایه‌گذاری در پیاده‌سازی و عملیاتی نمودن کنترل‌ها و خسارات احتمالی ناشی از رخدادهای امنیت اطلاعات برقرار شود؛

کنترل‌های مشخص‌شده در استاندارد ISO/IEC 27002 بهترین اقدامات قابل‌اعمال در بیشتر سازمان‌ها قلمداد و به آسانی با سازمان‌های دارای اندازه‌ها و پیچیدگی‌های مختلف منطبق می‌شوند. سایر استانداردهای خانواده ISMS، راهنمایی در مورد انتخاب و به‌کارگیری کنترل‌های ISO/IEC 27002 برای سیستم مدیریت امنیت اطلاعات فراهم می‌کنند.

توصیه می‌شود کنترل‌های امنیت اطلاعات در مرحله مشخص‌سازی و طراحی الزامات سیستم‌ها و پروژه‌ها در نظر گرفته شود. کوتاهی در چنین کاری می‌تواند منجر به راه‌حل‌های ناکارآمدتر و پرهزینه‌تر شده و در بدترین حالت ممکن است به عدم توانایی در تحقق امنیت مناسب شود. کنترل‌ها می‌توانند از ISO/IEC 27002 یا سایر مجموعه کنترل‌ها انتخاب شده، یا می‌تواند مجموعه جدیدی از کنترل‌ها برای برآورده سازی نیازهای خاص سازمان طراحی شود. ضروری است که تشخیص داده شود، برخی از کنترل‌ها ممکن است برای هر سیستم یا محیط اطلاعاتی قابل به کارگیری نباشد و ممکن است برای همه سازمان‌ها قابلیت به کارگیری نداشته باشد.

بعضی مواقع، زمان پیاده‌سازی مجموعه کنترل‌های انتخاب‌شده طولانی شده و در طی این مدت، سطح مخاطره از مقداری که می‌توان در بلند مدت تحمل کرد، بیشتر می‌شود، توصیه می شود، معیار مخاطره، پوشش‌دهنده قابلیت پذیرش مخاطرات بر اساس بازه‌های زمانی کوتاهی که کنترل‌ها مستقر می‌شوند، باشد. در بازه‌های زمانی مختلف، مادامی‌که پیاده‌سازی کنترل‌ها در حال پیشرفت است، طرف‌های علاقه‌مند باید از سطوح مخاطره‌ای که برآورد یا پیش‌بینی‌شده است، مطلع شوند.

باید توجه داشت که هیچ مجموعه‌ای از کنترل‌ها منجر به تحقق کامل امنیت اطلاعات نمی‌شود، بلکه توصیه می شود اقدامات مدیریتی بیشتری جهت پایش، ارزشیابی، بهبود کارایی و اثربخشی کنترل‌های امنیت اطلاعات جهت حمایت از اهداف سازمان پیاده‌سازی شود.

توصیه می‌شود، انتخاب و پیاده‌سازی کنترل‌ها در سند بیانیه کاربردپذیری مستند شود تا به الزامات انطباق کمک کند.

۳-۵-۶ پایش، نگهداری و بهبود اثربخشیISMS

سازمان نیاز به نگهداری و بهبود ISMS از طریق پایش و ارزشیابی عملکرد آن براساس خط‌مشی و اهداف سازمان و گزارش نتایج به مدیریت جهت بازنگری دارد. این بازنگریISMS، بررسی می‌کند که ISMS دربرگیرنده کنترل‌های مشخص برای برطرف سازی مخاطرات درون محدوده کاربرد ISMS است. علاوه بر این، بر مبنای سوابق نواحی پایش‌شده، شواهدی برای درستی‌سنجی و ردگیری اقدامات اصلاحی، پیشگیرانه و بهبوددهنده فراهم می‌کند.

۳-۵-۷ بهبود مستمر

هدف از بهبود مستمر ISMS افزایش احتمال دستیابی به اهدافی است که به حفظ محرمانگی، دسترس‌پذیری و جامعیت اطلاعات مرتبط است. تمرکز بهبود مستمر بر یافتن فرصت‌های بهبود است و بر این فرض مبتنی نیست که فعالیت‌های مدیریتی موجود به‌اندازه کافی خوب هستند یا به‌اندازه‌ای که در توان دارند، خوب هستند.

فعالیت‌های بهبود شامل موارد زیر است:

الف- تحلیل و ارزشیابی وضعیت موجود جهت تعیین نواحی بهبود؛

ب- ایجاد اهداف بهبود؛

پ- جستجو راه‌حل‌های ممکن جهت دستیابی به اهداف؛

ت- ارزشیابی راه‌حل‌های موجود و انتخاب راه‌حل؛

ث- پیاده‌سازی راه‌حل انتخاب‌شده؛

ج- سنجش، وارسی، تحلیل، ارزشیابی نتایج پیاده‌سازی جهت تعیین اینکه اهداف محقق شده‌اند؛

ج- قاعده‌مند سازی تغییرات.

نتایج در صورت نیاز، جهت فرصت‌های بهبود بیشتر، بازنگری می‌شود. بدین طریق، بهبود یک فعالیت مستمراست، به‌عبارت‌دیگر اقدامات به‌صورت متناوب تکرار می‌شود. بازخورد مشتریان و سایر طرف‌های علاقه‌مند، ممیزی‌ها و بازنگری سیستم مدیریت امنیت اطلاعات می‌تواند برای شناسایی فرصت‌های بهبود به کار گرفته شود.

۳-۶ عوامل مهم موفقیت ISMS

عوامل زیادی در پیاده‌سازی موفق ISMS مؤثرند تا سازمان را دررسیدن به اهداف کسب وکار خود یاری دهند. نمونه‌هایی از عوامل مهم موفقیت عبارت‌اند از:

الف- خط‌مشی ، اهداف و فعالیت‌های امنیت اطلاعات همسو با اهداف؛

ب- رویکرد و چارچوبی برای طراحی، پیاده‌سازی، پایش، نگهداری و بهبود امنیت اطلاعات سازگار با فرهنگ سازمانی؛

پ- پشتیبانی و پایبندی علنی ازطرف تمامی سطوح مدیریت به‌خصوص مدیریت ارشد؛

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

ث- برنامه‌ی مؤثر آگاه‌سازی، آموزش‌های حرفه‌ای و تحصیلی امنیت اطلاعات، به‌منظور ارتقای سطح آگاهی کارکنان و سایر طرف‌های مرتبط و الزامات امنیت اطلاعات که در خط مشی ها و استانداردهای امنیت اطلاعات مندرج شده و تشویق آن‌ها به رعایت این الزامات؛

ج- فرآیند مدیریت مؤثر رخداد امنیت اطلاعات؛

چ- رویکرد مؤثر مدیریت تداوم کسب‌وکار؛

ح- سیستم سنجش جهت ارزیابی عملکرد مدیریت امنیت اطلاعات و پیشنهادات بازخوردی برای بهبود عملکرد.

ISMS، احتمال دستیابی پایدار سازمان به عوامل اصلی موفقیت موردنیاز برای حفاظت دارایی‌های اطلاعاتی را افزایش می‌دهد.

۳-۷ مزایای استانداردهای خانواده ISMS

مزایای پیاده‌سازی ISMS عمدتاً ناشی از کاهش مخاطرات امنیت اطلاعات (مانند کاهش احتمال و/یا اثر ایجادشده توسط رخدادهای امنیت اطلاعات) است. به طور خاص، جهت دستیابی به موفقیت پایدار که از پذیرش استانداردهای خانواده ISMS ناشی می شود، مزایایی که برای سازمان‌ها محقق خواهد شد، عبارت‌اند از:

الف- چارچوب ساخت‌یافته جهت پشتیبانی از فرآیند مشخص‌سازی، پیاده‌سازی، بهره‌برداری و نگهداری ISMS یکپارچه، مقرون‌به‌صرفه‌ی جامع، ارزش‌آفرین و همسو که نیازهای سازمان را در بهره‌برداری‌ها و جایگاه‌های مختلف برآورده می‌کند؛

ب- یاری مدیران جهت مدیریت و عملیاتی سازی سازگار رویکردهای مدیریت امنیت اطلاعات با یک رفتار مسئولانه در بستر مدیریت و حاکمیت بر مخاطره، شامل آموزش و یادگیری صاحبان سیستم و کسب‌وکار در مورد مدیریت کلان نگر[1] امنیت اطلاعات؛

پ- ترویج اقدامات امنیت اطلاعات مطلوب و پذیرفته‌شده‌ی جهانی، با روش غیردستوری و آزادی عمل دادن به سازمان‌ها در پذیرش و بهبود کنترل‌های مرتبط با شرایط خاص آن‌ها که منطبق شود و به‌منظور نگهداری از آن‌ها در برابر تغییرات داخلی و خارجی؛ و

ت- تدارک زبان مشترک و مفاهیم پایه‌ای برای امنیت اطلاعات و کمک به ایجاد اطمینان در شرکای کاری در مورد ISMS موردتوافق، به‌خصوص اگر خواهان دریافت گواهی رعایت استاندارد ISO/IEC27001 از نهاد معتبر صدور گواهی[2] باشند؛

ث- افزایش اعتماد ذی‌نفعان به سازمان؛

ج- تحقق نیازها و انتظارات اجتماعی؛

چ- مدیریت اقتصادی کارآمدتر سرمایه‌گذاری‌های امنیت اطلاعات.

۴ استانداردهای خانواده ISMS

۴-۱ اطلاعات کلی

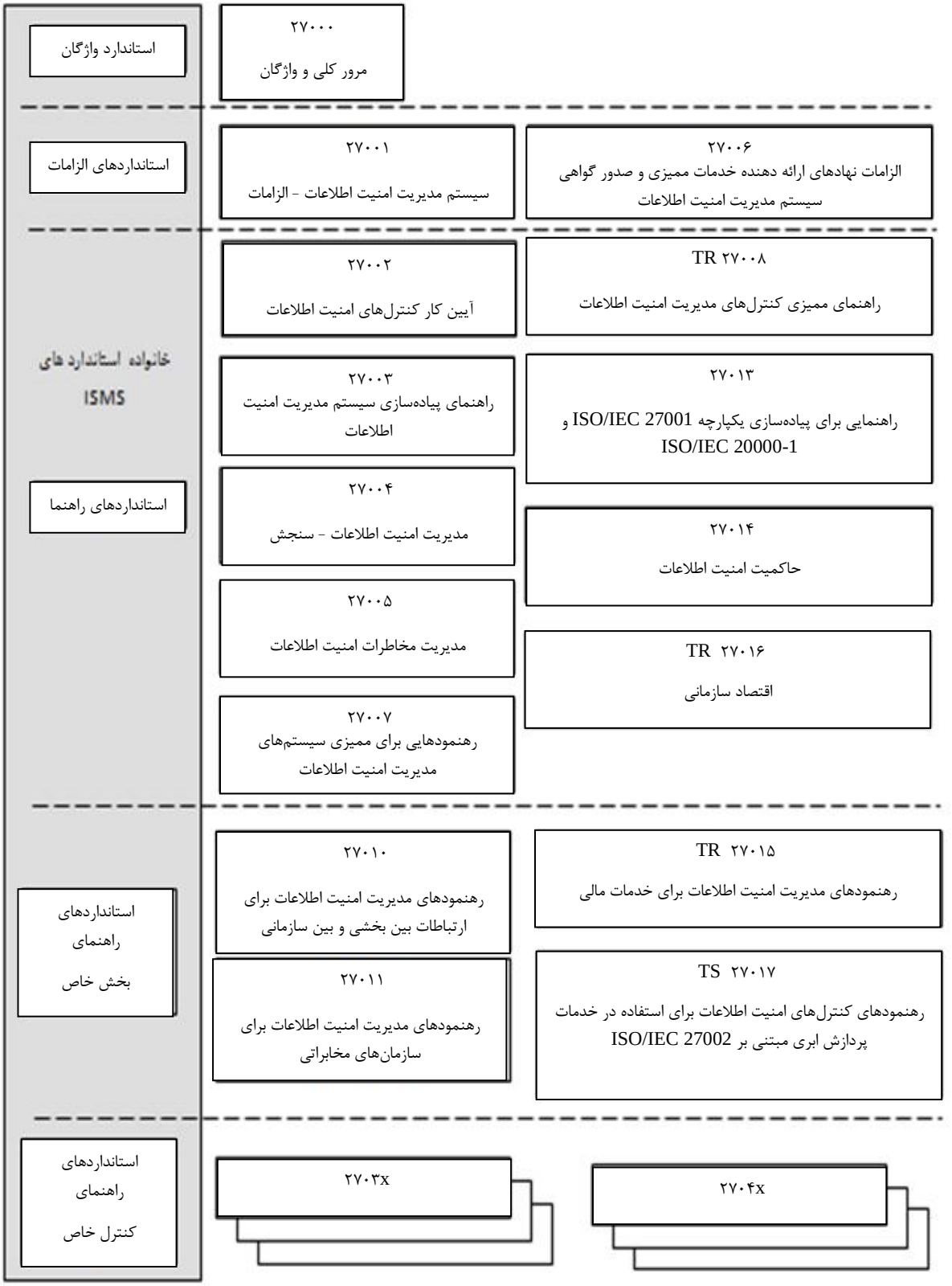
استانداردهای خانواده ISMS شامل استانداردهای مرتبط باهم است که درگذشته منتشرشده‌اند یا در دست تدوین هستند و تعدادی از مؤلفه‌های ساختاری مهم را در برمی‌گیرند. این مؤلفه‌ها متمرکز براستانداردهایی اجباری است که به توصیف الزامات ISMS (استانداردISO/IEC 27001) و همچنین الزامات نهاد صدور گواهی (استانداردISO/IEC27006) که انطباق با استاندارد ISO/IEC 27001 را تایید می‌کنند، به کار گرفته می‌شوند. سایر استانداردها، راهنمایی برای جنبه‌های مختلف پیاده‌سازیISMS، پرداختن به فرآیند عمومی، رهنمودهای مرتبط با کنترل و راهنمایی‌های بخش‌های خاص را فراهم می‌کند.

روابط استانداردهای خانواده ISMS در شکل ۱ نشان داده‌شده است.

الف- هر یک از استانداردهای خانواده ISMS برحسب نوع (یا نقش) آن در خانواده استانداردهای ISMS و شماره مراجع آن، در ادامه شرح داده‌شده است. بندهای کاربردپذیر عبارت‌اند از: استانداردهای توصیف کننده مرورکلی و واژگان (طبق بند ۴-۲)؛

1 - Holistic
2 - Accredited Certification Body

ب- استانداردهای مشخص‌کننده الزامات (طبق بند ۴-۳)؛
پ- استانداردهای توصیف‌کننده راهنماهای کلی (طبق بند ۴-۴)؛ یا
ت- استانداردهای توصیف‌کننده راهنماهای بخشی خاص (طبق بند ۴-۵).



شکل ۱: ارتباط استانداردهای خانواده ISMS

۴-۲ استانداردهای توصیف‌کننده مرورکلی و واژگان

۴-۲-۱ استاندارد ISO/IEC 27000 (این سند)

فناوری اطلاعات- فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات- مرورکلی و واژگان

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

الف- مرورکلی بر استانداردهای خانواده ISMS؛

ب- مقدمه‌ای بر سیستم‌های مدیریت امنیت اطلاعات (ISMS)؛ و

پ- اصطلاحات و تعاریف مورداستفاده در همه استانداردهای خانواده ISMS.

هدف: ISO/IEC 27000 مبانی سیستم‌های مدیریت امنیت اطلاعات را که موضوع استانداردهای خانواده ISMS است، توصیف کرده و اصطلاحات مرتبط را تعریف می‌کند.

۴-۳ استانداردهای مشخص‌کننده الزامات

۴-۳-۱ استاندارد ISO/IEC 27001[1]

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

دامنه کاربرد: این استاندارد ملی الزامات استقرار، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود سیستم‌های رسمی مدیریت امنیت اطلاعات (ISMS) با درنظرگرفتن محتوای مخاطرات کلی کسب‌وکار سازمان را مشخص می‌کند. این استاندارد همچنین الزامات پیاده‌سازی کنترل‌های امنیتی که با نیازهای سازمان‌های مختلف یا بخش‌های وابسته به آن منطبق شده است را مشخص می‌کند. این استاندارد ملی، می تواند برای همه سازمان‌ها صرف‌نظر از نوع و اندازه و ماهیت، مورد استفاده قرار گیرد.

هدف: استاندارد ISO/IEC 27001 الزامات اجباری توسعه و بهره‌برداری از ISMS شامل مجموعه کنترل‌هایی به‌منظور کنترل و برخورد با مخاطرات مرتبط با دارایی‌های اطلاعاتی را که سازمان با کمک ISMS از آن‌ها حفاظت می‌کند، ارائه می‌دهد. سازمان‌هایی که ISMS در آن‌ها عملیاتی است، ممکن است انطباقشان، ممیزی و گواهی‌شده باشند. اهداف کنترلی و کنترل‌های پیوست الف (استاندارد ISO/IEC 27001) باید به‌عنوان قسمتی از این فرآیند ISMS انتخاب شوند تا الزامات شناسایی‌شده را به‌طور مناسب پوشش دهند. اهداف کنترلی و کنترل‌های فهرست شده در جدول الف (استاندارد ISO/IEC 27001) به‌طور مستقیم از بندهای ۵ تا ۱۸ استاندارد ISO/IEC 27002 استخراج‌شده و با آن‌ها هم‌راستا است.

۱- استاندارد ملی ایران با شماره ISIRI ISO/IEC 27001 در سال ۱۳۹۴ با منبع بین‌المللی ISO/IEC 27001:2013 منتشر شده است.

۲-۳-۴ استاندارد ISO/IEC 27006[1]

فناوری اطلاعات- فنون امنیتی- الزامات نهادهای ارائه‌دهنده خدمات ممیزی و صدور گواهی‌نامه‌های مدیریت امنیت اطلاعات

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

هدف: استاندارد ملی ایران شماره ISO/IEC 27006 مکمل ISO/IEC 17021 در ارائه الزاماتی که توسط آن‌ها سازمان‌های صدور گواهی، اعتبارسنجی می شوند، است، بنابراین به این سازمان‌ها اجازه می‌دهد تا گواهی انطباق مستمر الزامات استاندارد ISO/IEC 27001 را صادر کنند.

۴-۴ استانداردهای توصیف‌کننده راهنماهای کلی

۱-۴-۴ استاندارد ISO/IEC 27002[2]

فناوری اطلاعات- فنون امنیتی- آیین کار کنترل‌های امنیت اطلاعات

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

هدف: استاندارد ISO/IEC 27002 راهنمایی پیاده‌سازی کنترل‌های امنیت اطلاعات را فراهم می‌آورد. به‌خصوص بندهای ۵ تا ۱۸، توصیه‌ها و راهنمایی‌های خاص پیاده‌سازی در مورد بهروش‌های پشتیبانی از کنترل‌های مشخص‌شده در بندهای الف-۵ تا الف-۱۸ ISO/IEC 27001 ارائه می‌دهد.

۲-۴-۴ استاندارد ISO/IEC 27003[3]

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

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

۱- استاندارد ملی ایران با شماره ISIRI ۲۷۰۰۶ در سال ۱۳۸۷ با منبع بین‌المللی ISO/IEC 27006:2007 منتشر شده است.

۲- استاندارد ملی ایران با شماره ISIRI ۲۷۰۰۵ در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27005:2011 منتشر شده است.

۳- استاندارد ملی ایران با شماره ISIRI ۲۷۰۰۳ در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27003:2010 منتشر شده است

هدف: استاندارد ملی ایران با شماره ۲۷۰۰۳ رویکرد فرآیندگرا برای پیاده‌سازی موفق ISMS بر اساس استاندارد ملی ایران شماره ۲۷۰۰۱ ارائه می‌کند.

۴-۴-۳ استاندارد ISO/IEC 27004[1]

فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات-سنجش

دامنه کاربرد: استاندارد ملی، راهنمایی و توصیه راجع به تدوین و به‌کارگیری سنجش به‌منظور ارزیابی اثربخشی ISMS، اهداف کنترلی و کنترل‌های استفاده‌شده در پیاده‌سازی و مدیریت امنیت اطلاعات همان‌طور که در استاندارد ملی ایران شماره ۲۷۰۰۱ مشخص‌شده را ارائه می‌کند.

هدف: استاندارد ملی ایران شماره ۱۴۰۹۶ چارچوبی برای سنجش ارائه کرده که ارزیابی اثربخشی ISMS که باید براساس استاندارد ملی ایران شماره ۲۷۰۰۱ اندازه گرفته شود را میسر کند.

۴-۴-۴ استاندارد ISO/IEC 27005[2]

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 ۲۷۰۰۱ را پشتیبانی می‌کند.

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

۴-۴-۵ استاندارد ISO/IEC 27007

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

دامنه کاربرد: این استاندارد ملی، (افزون بر راهنمایی ارائه‌شده در استاندارد ملی ایران شماره ۱۹۰۱۱: سال ۱۳۹۲ است که به‌طورکلی در سیستم‌های مدیریتی کاربردپذیر است)، راهنمایی را برای انجام ممیزی ISMS و نیز راهنمایی بر شایستگی ممیزان سیستم مدیریت امنیت اطلاعات ارائه می‌کند.

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

۱- استاندارد ملی ایران با شماره ISIRI ۱۴۰۹۶ در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27004:2009 منتشر شده است.

۲- استاندارد ملی ایران با شماره ISIRI ۲۷۰۰۵ در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27005:2011 منتشر شده است.

۶-۴-۴ استاندارد ISO/IEC TR27008

فناوری اطلاعات- فنون امنیتی- راهنماهایی برای ممیزان کنترل‌های مدیریت امنیت اطلاعات

دامنه کاربرد: این گزارش فنی راهنمایی برای بازنگری پیاده‌سازی و عملیاتی سازی کنترل‌ها، شامل بررسی انطباق فنی کنترل‌های سیستم اطلاعاتی در انطباق با استانداردهای امنیت اطلاعات مستقرشده سازمان ارائه می‌کند.

هدف: این گزارش فنی تمرکز بر بازنگری‌های کنترل‌های امنیت اطلاعات که شامل بررسی انطباق فنی با استاندارد پیاده‌سازی امنیت اطلاعات که توسط سازمان مستقر شده است، ارائه می دهد. این گزارش قصد ندارد راهنمایی خاصی در مورد بررسی انطباق در ارتباط با سنجش، ارزیابی مخاطره یا ممیزی ISMS چنانکه در استانداردهای ISO/IEC 27004 یا ISO/IEC 27005 یا ISO/IEC 27007 مشخص‌شده است، ارائه کند. این گزارش فنی به قصد ممیزی‌های سیستم‌های مدیریتی نیست.

۷-۴-۴ استاندارد ISO/IEC 27013

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

دامنه کاربرد: این استاندارد بین‌المللی راهنمای جهت پیاده‌سازی یکپارچه ISO/IEC 27001 و ISO/IEC 20000-1 برای سازمان‌هایی فراهم می‌کند که قصد دارند:

الف- درحالی‌که انطباق با ISO/IEC 20000-1 پذیرفته‌شده است، ISO/IEC 27001 را پیاده‌سازی کنند، یا بالعکس؛

ب- هر دو استاندارد ISO/IEC 27001 وISO/IEC 20000-1 را با یکدیگر پیاده‌سازی کنند؛

پ- پیاده‌سازی‌های سیستم مدیریتی ISO/IEC 27001 و ISO/IEC 20000-1 را هم‌راستا کنند.

هدف: درک بهتری از مشخصه‌ها، شباهت‌ها و تفاوت‌های ISO/IEC 27001 وISO/IEC 20000-1 برای سازمان ارائه کند که به طرح‌ریزی سیستم یکپارچه‌ای که منطبق بر هر دو استاندارد باشد کمک کند.

۸-۴-۴ استاندارد ISO/IEC 27014

فناوری اطلاعات- فنون امنیتی- حاکمیت امنیت اطلاعات

دامنه کاربرد: این استاندارد بین‌المللی راهنمایی، جهت اصول و فرآیندهای حاکمیت فناوری اطلاعات فراهم می‌آورد که به‌واسطه آن سازمان می‌تواند مدیریت امنیت اطلاعات را ارزشیابی، هدایت و پایش کند.

هدف: امنیت اطلاعات به موضوعی کلیدی برای سازمان‌ها تبدیل‌شده است. نه‌تنها الزامات قراردادی بلکه نقص معیارهای امنیت اطلاعات سازمان می‌تواند تأثیر مستقیمی بر شهرت سازمان داشته باشد. بنابراین هیأت حاکم، به‌عنوان بخشی از وظایف حکومتی خود، به شکل فزاینده‌ای نیازمند نظارت بر امنیت اطلاعات است تا از تحقق اهداف سازمان اطمینان حاصل کند.

۹-۴-۴ استاندارد ISO/IEC TR 27016

فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- اقتصاد سازمانی

دامنه کاربرد: این گزارش فنی روشی برای سازمان‌ها فراهم می‌آورد که آن‌ها را قادر می‌سازد تا درک اقتصادی بهتری به دست آورند از اینکه چگونه با دقت بیشتری ارزش دارایی‌های اطلاعاتی شناسایی‌شده خود را تعیین کنند؛ ارزش مخاطرات بالقوه چنین دارایی‌ها را تعیین کنند؛ ارزشی که کنترل های حفاظت اطلاعات برای این دارایی های اطلاعاتی دارند را درک کنند و سطح بهینه منابعی را که جهت امن سازی این دارایی‌ها باید به کار گرفته شود مشخص کنند.

هدف: این گزارش فنی، استانداردهای خانواده ISMS را از طریق پوشش دادن جنبه اقتصادی در حفاظت از دارایی‌های اطلاعاتی سازمان در یک گستره وسیع‌تر اجتماعی که سازمان در آن فعالیت می‌کند، تکمیل می کند. این کار از طریق راهنمایی جهت چگونگی به‌کارگیری اقتصاد سازمانی امنیت اطلاعات از طریق استفاده از مدل‌ها و مثال‌ها، فراهم می‌شود.

۵-۴ استانداردهای توصیف‌کننده راهنماهای بخش خاص

۱-۵-۴ استاندارد ISO/IEC 27010

فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات برای ارتباطات بین‌بخشی و بین سازمانی

دامنه کاربرد: این استاندارد بین المللی علاوه بر راهنمایی‌های ارائه‌شده در خانواده استانداردهای ISO/IEC 27000، راهنمایی‌هایی جهت پیاده‌سازی مدیریت امنیت اطلاعات در جوامع اشتراک‌گذار اطلاعات ارائه کرده و همچنین کنترل‌ها و راهنمایی‌های ویژه‌ای جهت راه‌اندازی، پیاده‌سازی، نگهداری و بهبود امنیت اطلاعات در ارتباطات بین‌بخشی و بین سازمانی فراهم کرده است.

هدف: این استاندارد بین المللی برای تمام اشکال تبادل و اشتراک اطلاعات حساس به‌صورت عمومی و خصوصی، ملی یا بین‌المللی، درون یک صنعت مشابه یا بخش بازار یا بین بخش‌های مختلف قابل به‌کارگیری است. به‌طور خاص، این استاندارد ممکن است برای تبادل و اشتراک اطلاعات مرتبط با تدارک، نگهداری و محافظت زیرساخت‌های حساس سازمان یا دولت، قابل به‌کارگیری باشد.

۲-۵-۴ استاندارد 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 پشتیبان پیاده‌سازی مدیریت امنیت اطلاعات در سازمان‌های مخابراتی را ارائه می‌کند.

۱- استاندارد ملی ایران با شماره ۲۷۰۱۱ ISIRI در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27011:2008 منتشر شده است.

هدف: استاندارد ملی ایران شماره ۲۷۰۱۱، نسخه‌ای سازگاریافته ازدستورالعمل‌های ISO/IEC 27002 بـرای سازمان‌های مخابراتی که مختص همان صنعت تنظیم‌شده است را ارائه می‌کند و اضافه بر الزاماتی اسـت کـه باید برای پاسخ به پیوست الف استاندارد ISO/IEC 27001 رعایت شوند.

۴-۵-۳ استاندارد ISO/IEC TR 27015[1]

فناوری اطلاعات- فنون امنیتی- راهنماهای مدیریت امنیت اطلاعات برای خدمات مالی

دامنه کاربرد: این گزارش فنی علاوه بر راهنمایی‌های ارائه‌شده در خانواده استانداردهای ISMS، راهنمایی-هایی جهت راه‌اندازی، پیاده‌سازی، نگهداری و بهبود امنیت در سازمان‌هایی که فـراهم‌کننـده خـدمات مـالی هستند، ارائه می‌کند.

هدف: این گزارش فنی مکمل اختصاصـی اسـتانداردهای بـین‌المللـی ISO/IEC 27001 و ISO/IEC 27002 جهت استفاده در سازمان‌هایی است که خدمات مالی ارائه می‌کنند و این سازمان‌ها را در موارد زیر پشتیبانی می‌کنند:

الف- راه‌اندازی، پیاده‌سازی، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات مبتنی بر استاندارد بین‌المللی ISO/IEC 27001:2005؛

ب- طراحی و پیاده‌سازی کنترل‌های تعریـف‌شـده در اسـتاندارد بـین‌المللـی ISO/IEC 27002:2005 یـا در استاندارد حاضر.

۴-۵-۴ استاندارد ISO 27799[2]

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

دامنه کاربرد: این استاندارد ملی، راهنماهای پشتیبانی‌کننده از پیـاده‌سـازی مـدیریت امنیـت اطلاعـات در سازمان‌های بهداشت را ارائه می‌کند.

هدف: استاندارد ملی ایران شماره ۱۳۲۲۰،نسخه‌ای سازگاریافته ازدستورالعمل‌های ISO/IEC 27002 برای سازمان‌های سلامت که مختص همان صنعت تنظیم‌شده است را ارائه می‌کند و اضافه بر الزاماتی است که باید برای پاسخ به پیوست A استاندارد ISO/IEC 27001 رعایت شوند.

۱- استاندارد ملی ایران با شماره ISIRI ۲۷۰۱۵ در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27015:2012 منتشر شده است.

۲- استاندارد ملی ایران با شماره ISIRI۱۳۲۲۰ در سال ۱۳۸۹ با منبع بین المللی ISO 27799:2008 ، منتشر شده است..

پیوست الف

(اطلاعاتی)

کاربرد افعال در بیان مقررات

هرکدام از مستندات استانداردهای خانواده ISMS به‌خودی‌خود تعهدی برای فردی ایجاد نمی‌کند. اما چنین تعهدی برای مثال ممکن است توسط مقررات یا قراردادی ایجاد شود. برای آن‌که 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 خانواده‌یISMS باشد را تصریح می‌کند.

جدول مبتنی بر مفاد پیوست H از قسمت دوم راهنمایی ISO/IEC با نام قواعد برای ساختار و پیش نویس استانداردهای بین المللی است.

نشانه	شرح
الزامات[a]	اصطلاحات«باید[b]» و«نباید[c]» دلالت بر الزاماتی دارد که به‌شدت دنبال می‌شوند تا مطابق با سند باشد و انحراف از آن مجاز نیست.
توصیه[d]	اصطلاحات«توصیه می‌شود[e]» و«توصیه نمی‌شود[f]» نشان‌دهنده این است که از میان چندین مورد ممکن، یک مورد به دلیل اینکه خصوصاً مناسب است، پیشنهاد می شود، بدون آن‌که به گزینه‌های دیگر اشاره یا آن‌ها را مستثنی کند یا این‌که عمل معینی برتری داده شود ولی نه اینکه حتما الزامی بوده یا که (به شکل منفی آن) امکان یا عمل معینی ناچیز انگاشته شود ولی منع نشده است.
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]» نشان‌دهنده امکان 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)
اصطلاح و مالکیت اصطلاح

ب-۱ مالکیت اصطلاح

مالک اصطلاح در مجموعه استانداردهای خانواده ۲۷۰۰۰، استانداردی است که اصطلاح را در ابتدا تعریف کرده است. مالک اصطلاح همچنین مسئولیت نگهداری اصطلاح را بر عهده دارد، ازجمله:

- ارائه،
- بازنگری،
- روزآمدی، و
- حذف.

یادآوری ۱-ISO/IEC27001 خود، هرگز به‌عنوان مالک اصطلاح تلقی نمی‌شود.

یادآوری ۲-ISO/IEC 27001 و ISO/IEC 27006 به‌عنوان استانداردهای پایه (به‌عبارت‌دیگر، دربرگیرنده الزامات) همیشه به‌عنوان مالک غالب اصطلاح، موردتوجه قرار می‌گیرند.

ب-۲ اصطلاحات مرتب‌شده بر اساس استانداردها	
ب-۲-۱ **ISO/IEC 27001**	
۲-۵ ممیزی	Audit
۲-۹ دسترس‌پذیری	Availability
۲-۱۱ شایستگی	Competence
۲-۱۲ محرمانگی	Confidentiality
۲-۱۳ انطباق	Conformity
۲-۱۵ بهبود مستمر	Continual improvement
۲-۱۶ کنترل	Control
۲-۱۸ اصلاح	Correction
۲-۱۹ اقدام اصلاحی	Corrective action
۲-۲۳ اطلاعات مستند	Documented information
۲-۲۴ اثربخشی	Effectiveness
۲-۳۳ امنیت اطلاعات	Information security

Integrity	۲-۴۰ یکپارچگی
Interested party	۲-۴۱ طرف‌علاقه‌مند
Management system	۲-۴۶ سیستم مدیریت
Measurement	۲-۴۸ سنجش
Monitoring	۲-۵۲ پایش
Non-conformity	۲-۵۳ عدم انطباق
Objective	۲-۵۶ هدف
Organization	۲-۵۷ سازمان
Outsource(verb)	۲-۵۸ برون‌سپاری کردن
Performance	۲-۵۹ عملکرد
Policy	۲-۶۰ خط‌مشی
Process	۲-۶۱ فرآیند
Requirement	۲-۶۳ الزام
Review	۲-۶۵ بازنگری
Risk	۲-۶۸ مخاطره
Risk owner	۲-۷۸ مالک مخاطره
Top management	۲-۸۴ مدیریت ارشد
	ب-۲-۲ **ISO/IEC 27002**
Access control	۲-۱ کنترل دسترسی
Attack	۲-۳ حمله
Authentication	۲-۷ اصالت‌سنجی
Authenticity	۲-۸ اصالت
Control objective	۲-۱۷ هدف کنترلی
Information processing facilities	۲-۳۲ تسهیلات پردازش اطلاعات
Information security continuity	۲-۳۴ تداوم امنیت اطلاعات

Information security event	۲-۳۵ رویداد امنیت اطلاعات
Information security incident	۲-۳۶ رخداد امنیت اطلاعات
Information security incident management	۲-۳۷ مدیریت رخداد امنیت اطلاعات
Information system	۲-۳۹ سیستم اطلاعاتی
Non-repudiation	۲-۵۴ سلب انکار
Reliability	۲-۶۲ اطمینان پذیری
	ب-۲-۳ **ISO/IEC 27003**
ISMS project	43-2 پروژه ISMS
	ب-۲-**4ISO/IEC 27004**
Analytical model	۲-۲ مدل تحلیلی
Attribute	۲-۴ صفت
Base measure	۲-۱۰ سنجه مبنا
Data	۲-۲۰ داده
Decision criteria	۲-۲۱ معیار تصمیم‌گیری
Derived measure	۲-۲۲ سنجه مشتق
Indicator	۲-۳۰ نشانگر
Information need	۲-۳۱ نیاز اطلاعاتی
Measure	۲-۴۷ سنجه
Measurement function	۲-۴۹ تابع سنجش
Measurement method	۲-۵۰ روش سنجش
Measurement results	۲-۵۱ نتایج سنجش
Object	۲-۵۵ شیء
Scale	۲-۸۰ مقیاس
Unit of measurement	۲-۸۶ واحد سنجش
Validation	۲-۸۷ اعتبارسنجی

Verification	۲-۸۸ درستی سنجی
	ب-۲-۵ **ISO/IEC 27005**
Consequence	۲-۱۴ پیامد
Event	۲-۲۵ رویداد
External context	۲-۲۷ زمینه‌ی بیرونی
Internal context	۲-۴۲ زمینه‌ی درونی
Level of risk	۲-۴۴ سطح مخاطره
Likelihood	۲-۴۵ فرصت وقوع
Residual risk	۲-۶۴ مخاطره باقیمانده
Risk acceptance	۲-۶۹ پذیرش مخاطره
Risk analysis	۲-۷۰ تحلیل مخاطره
Risk assessment	۲-۷۱ ارزیابی مخاطره
Risk communication and consultation	۲-۷۲ اطلاع‌رسانی و مشاوره مخاطره
Risk criteria	۲-۷۳ معیار مخاطره
Risk evaluation	۲-۷۴ ارزشیابی مخاطره
Risk identification	۲-۷۵ شناسایی مخاطره
Risk management	۲-۷۶ مدیریت مخاطره
Risk management process	۲-۷۷ فرآیند مدیریت مخاطره
Risk treatment	۲-۷۹ برطرف سازی مخاطره
Threat	۲-۸۳ تهدید
Vulnerability	۲-۸۹ آسیب‌پذیری
	ب-۲-۶ **ISO/IEC 27006**
Certificate	گواهی‌نامه
Certification body	نهاد صدور گواهی
Certification document	سند گواهی‌نامه

Mark	علامت
Organization	سازمان
	ب-۲-۷ **ISO/IEC 27007**
Audit scope	۲-۶ محدوده کاربرد ممیزی
	ب-۲-۸ **ISO/IEC TR 27008**
Review object	۲-۶۶ شیء موردبازنگری
Review objective	۲-۶۷ هدف بازنگری
Security implementation standard	۲-۸۱ استاندارد پیاده‌سازی امنیت
	ب-۲-۹ **ISO/IEC 27010**
Information sharing community	۲-۳۸ جامعه اشتراک‌گذار اطلاعات
Trusted information communication entity	۲-۸۵ هستار مورد اعتماد ارتباط اطلاعات
	ب-۲-۱۰ **ISO/IEC 27011**
Collocation	باهم گذاری
Communication centre	مرکز ارتباط
Essential communications	ارتباطات ضروری
Non-disclosure of communications	عدم افشاء ارتباطات
Personalinformation	اطلاعات شخصی
Perority call	تماس اولویت‌دار
Telecommunications applications	کاربردهای مخابراتی
Telecommunications business	کسب‌وکار مخابراتی
Telecommunications equipment room	اتاق تجهیزات مخابراتی
Telecommunications facilities	تسهیلات مخابراتی
Telecommunications organizations	سازمان‌های مخابراتی
Telecommunications records	سوابق مخابراتی
Telecommunications services	خدمات مخابراتی

Telecommunications service customer	مشتری خدمت مخابراتی
Telecommunications service user	کاربر خدمت مخابراتی
Terminal facilities	تسهیلات پایانه
User	کاربر
	ب-۲-۱۱ **ISO/IEC 27014**
Executive management	۲-۲۶ مدیریت اجرایی
Governance of information security	۲-۲۸ حاکمیت امنیت اطلاعات
Governing body	۲-۲۹ نهاد حکومتی
Stakeholder	۲-۸۲ ذینفع
	ب-۲-۱۲ **ISO/IEC TR 27015**
Financial services	خدمات مالی
	ب-۲-۱۳ **ISO/IEC 27016**
Annualized loss expectancy ALE	زیان سالانه مورد انتظار
direct value	ارزش مستقیم
Economic comparison	مقایسه اقتصادی
Economic factor	عامل اقتصادی
Economic justification	توجیه اقتصادی
Economic value added	ارزش‌افزوده اقتصادی
Economics	اقتصادی
Expected value	ارزش مورد انتظار
Extended value	ارزش تمدیدشده
Indirect value	ارزش غیرمستقیم
Information security economics	اقتصاد امنیت اطلاعات
Information security management IMS	مدیریت امنیت اطلاعات
Loss	زیان

Market value	ارزش بازار
Net present value	ارزش فعلی خالص
Non economic benefit	مزیت غیراقتصادی
Present value	ارزش فعلی
Opportunity cost	هزینه فرصت
Opportunity value	ارزش فرصت
Regulatory requirements	الزامات قراردادی
Return on investment	نرخ بازگشت سرمایه
Societal value	ارزش اجتماعی
Value	ارزش
Value-at-risk	ارزش در معرض مخاطره

به ترتیب الفبای فارسی	ب-۲ اصطلاحات مرتب‌شده بر اساس استانداردها
	ب-۲-۱ **ISO/IEC 27001**
Effectiveness	۲-۲۴ اثربخشی
Correction	۲-۱۸ اصلاح
Documented information	۲-۲۳ اطلاعات مستند
Corrective action	۲-۱۹ اقدام اصلاحی
Requirement	۲-۶۳ الزام
Information security	۲-۳۳ امنیت اطلاعات
Conformity	۲-۱۳ انطباق
Review	۲-۶۵ بازنگری
Outsource(verb)	۲-۵۸ برون‌سپاری کردن
Continual improvement	۲-۱۵ بهبود مستمر
Monitoring	۲-۵۲ پایش
Policy	۲-۶۰ خط‌مشی
Availability	۲-۹ دسترس‌پذیری
Organization	۲-۵۷ سازمان
Measurement	۲-۴۸ سنجش
Management system	۲-۴۶ سیستم مدیریت
Competence	۲-۱۱ شایستگی
Interested party	۲-۴۱ طرف‌علاقه‌مند
Non-conformity	۲-۵۳ عدم انطباق
Performance	۲-۵۹ عملکرد
Process	۲-۶۱ فرآیند
Control	۲-۱۶ کنترل
Risk owner	۲-۷۸ مالک مخاطره

Confidentiality	۲-۱۲ محرمانگی
Risk	۲-۶۸ مخاطره
Top management	۲-۸۴ مدیریت ارشد
Audit	۲-۵ ممیزی
Objective	۲-۵۶ هدف
Integrity	۲-۴۰ یکپارچگی
	ب-۲-۲ **ISO/IEC 27002**
Authenticity	۲-۸ اصالت
Authentication	۲-۷ اصالت‌سنجی
Non-repudiation	۲-۵۴ سلب انکار
Information security continuity	۲-۳۴ تداوم امنیت اطلاعات
Information processing facilities	۲-۳۲ تسهیلات پردازش اطلاعات
Attack	۲-۳ حمله
Information security incident	۲-۳۶ رخداد امنیت اطلاعات
Information security event	۲-۳۵ رویداد امنیت اطلاعات
Information system	۲-۳۹ سیستم اطلاعاتی
Reliability	۲-۶۲ اطمینان پذیری
Access control	۲-۱ کنترل دسترسی
Information security incident management	۲-۳۷ مدیریت رخداد امنیت اطلاعات
Control objective	۲-۱۷ هدف کنترلی
	ب-۲-۳ **ISO/IEC 27003**
ISMS project	43-2 پروژه ISMS
	ب-۲-**4ISO/IEC 27004**
Validation	۲-۸۷ اعتبارسنجی
Measurement function	۲-۴۹ تابع سنجش

Data	۲-۲۰ داده
Verification	۲-۸۸ درستی سنجی
Measurement method	۲-۵۰ روش سنجش
Derived measure	۲-۲۲ سنجه مشتق
Base measure	۲-۱۰ سنجه مبنا
Object	۲-۵۵ شیء
Attribute	۲-۴ صفت
Analytical model	۲-۲ مدل تحلیلی
Decision criteria	۲-۲۱ معیار تصمیم‌گیری
Measure	۲-۴۷ سنجه
Scale	۲-۸۰ مقیاس
Measurement results	۲-۵۱ نتایج سنجش
Indicator	۲-۳۰ نشانگر
Information need	۲-۳۱ نیاز اطلاعاتی
Unit of measurement	۲-۸۶ واحد سنجش
	ب-۲-۵ **ISO/IEC 27005**
Risk evaluation	۲-۷۴ ارزشیابی مخاطره
Risk assessment	۲-۷۱ ارزیابی مخاطره
Vulnerability	۲-۸۹ آسیب‌پذیری
Risk communication and consultation	۲-۷۲ اطلاع‌رسانی و مشاوره مخاطره
Risk treatment	۲-۷۹ برطرف سازی مخاطره
Risk acceptance	۲-۶۹ پذیرش مخاطره
Consequence	۲-۱۴ پیامد
Risk analysis	۲-۷۰ تحلیل مخاطره
Threat	۲-۸۳ تهدید

Event	۲-۲۵ رویداد
External context	۲-۲۷ زمینه‌ی بیرونی
Internal context	۲-۴۲ زمینه‌ی درونی
Level of risk	۲-۴۴ سطح مخاطره
Risk identification	۲-۷۵ شناسایی مخاطره
Risk management process	۲-۷۷ فرآیند مدیریت مخاطره
Likelihood	۲-۴۵ فرصت وقوع
Residual risk	۲-۶۴ مخاطره باقیمانده
Risk management	۲-۷۶ مدیریت مخاطره
Risk criteria	۲-۷۳ معیار مخاطره
	ب-۲-۶ **ISO/IEC 27006**
Organization	سازمان
Certification document	سند گواهی‌نامه
Mark	علامت
Certificate	گواهی‌نامه
Certification body	نهاد صدور گواهی
	ب-۲-۷ **ISO/IEC 27007**
Audit scope	۲-۶ محدوده کاربرد ممیزی
	ب-۲-۸ **ISO/IEC TR 27008**
Security implementation standard	۲-۸۱ استاندارد پیاده‌سازی امنیت
Review object	۲-۶۶ شیء موردبازنگری
Review objective	۲-۶۷ هدف بازنگری
	ب-۲-۹ **ISO/IEC 27010**
Information sharing community	۲-۳۸ جامعه اشتراک‌گذار اطلاعات
Trusted information communication entity	۲-۸۵ هستار مورد اعتماد ارتباط اطلاعات

	ب-۲-۱۰ **ISO/IEC 27011**
Telecommunications equipment room	اتاق تجهیزات مخابراتی
Essential communications	ارتباطات ضروری
Personalinformation	اطلاعات شخصی
Collocation	باهم گذاری
Terminal facilities	تسهیلات پایانه
Telecommunications facilities	تسهیلات مخابراتی
Perority call	تماس اولویت‌دار
Telecommunications services	خدمات مخابراتی
Telecommunications organizations	سازمان‌های مخابراتی
Telecommunications records	سوابق مخابراتی
Non-disclosure of communications	عدم افشاء ارتباطات
User	کاربر
Telecommunications service user	کاربر خدمت مخابراتی
Telecommunications applications	کاربردهای مخابراتی
Telecommunications business	کسب‌وکار مخابراتی
Communication centre	مرکز ارتباط
Telecommunications service customer	مشتری خدمت مخابراتی
	ب-۲-۱۱ **ISO/IEC 27014**
Governance of information security	۲-۲۸ حاکمیت امنیت اطلاعات
Stakeholder	۲-۸۲ ذینفع
Executive management	۲-۲۶ مدیریت اجرایی
Governing body	۲-۲۹ نهاد حکومتی
	ب-۲-۱۲ **ISO/IEC TR 27015**
Financial services	خدمات مالی

	ب-۲-۱۳ **ISO/IEC 27016**
Value	ارزش
Societal value	ارزش اجتماعی
Economic value added	ارزش‌افزوده اقتصادی
Market value	ارزش بازار
Extended value	ارزش تمدیدشده
Value-at-risk	ارزش در معرض مخاطره
Indirect value	ارزش غیرمستقیم
Opportunity value	ارزش فرصت
Present value	ارزش فعلی
Net present value	ارزش فعلی خالص
direct value	ارزش مستقیم
Expected value	ارزش مورد انتظار
Information security economics	اقتصاد امنیت اطلاعات
Economics	اقتصادی
Regulatory requirements	الزامات قراردادی
Economic justification	توجیه اقتصادی
Loss	زیان
Annualized loss expectancy ALE	زیان سالانه مورد انتظار
Economic factor	عامل اقتصادی
Information security management IMS	مدیریت امنیت اطلاعات
Non economic benefit	مزیت غیراقتصادی
Economic comparison	مقایسه اقتصادی
Return on investment	نرخ بازگشت سرمایه
Opportunity cost	هزینه فرصت

پیوست پ
(اطلاعاتی)
واژگان برحسب شماره بندها

ردیف	شماره بند	واژگان فارسی	واژگان انگلیسی	شماره صفحه
۱	۲-۱	کنترل دسترسی	access control	۱
۲	۲-۲	مدل تحلیلی	analytical model	۱
۳	۲-۳	حمله	attack	۱
۴	۲-۴	صفت	attribute	۲
۵	۲-۵	ممیزی	audit	۲
۶	۲-۶	محدوده ممیزی	audit scope	۲
۷	۲-۷	اصالت‌سنجی	authentication	۲
۸	۲-۸	اصالت	authenticity	۲
۹	۲-۹	دسترس‌پذیری	availability	۲
۱۰	۲-۱۰	سنجه مبنا	base measure	۳
۱۱	۲-۱۱	شایستگی	competence	۳
۱۲	۲-۱۲	محرمانگی	confidentiality	۳
۱۳	۲-۱۳	انطباق	conformity	۳
۱۴	۲-۱۴	پیامد	consequence	۳
۱۵	۲-۱۵	بهبود مستمر	continual improvement	۳
۱۶	۲-۱۶	کنترل	control	۴
۱۷	۲-۱۷	هدف کنترلی	control objective	۴
۱۸	۲-۱۸	اصلاح	correction	۴
۱۹	۲-۱۹	اقدام اصلاحی	corrective action	۴
۲۰	۲-۲۰	داده	data	۴

ردیف	شماره بند	واژگان فارسی	واژگان انگلیسی	شماره صفحه
۲۱	۲-۲۱	معیار تصمیم‌گیری	decision criteria	۴
۲۲	۲-۲۲	سنجه مشتق	derived measure	۵
۲۳	۲-۲۳	اطلاعات مستند	documented information	۵
۲۴	۲-۲۴	اثربخشی	effectiveness	۵
۲۵	۲-۲۵	رویداد	event	۵
۲۶	۲-۲۶	مدیریت اجرایی	executive management	۶
۲۷	۲-۲۷	زمینهٔ بیرونی	external context	۶
۲۸	۲-۲۸	حاکمیت امنیت اطلاعات	governance of information security	۶
۲۹	۲-۲۹	هیأت حاکم	governing body	۶
۳۰	۲-۳۰	نشانگر	indicator	۷
۳۱	۲-۳۱	نیاز اطلاعاتی	information need	۷
۳۲	۲-۳۲	تسهیلات پردازش اطلاعات	information processing facilities	۷
۳۳	۲-۳۳	امنیت اطلاعات	information security	۷
۳۴	۲-۳۴	تداوم امنیت اطلاعات	information security continuity	۷
۳۵	۲-۳۵	رویداد امنیت اطلاعات	information security event	۷
۳۶	۲-۳۶	رخداد امنیت اطلاعات	information security incident	۷
۳۷	۲-۳۷	مدیریت رخداد امنیت اطلاعات	information security incident management	۸
۳۸	۲-۳۸	جامعه اشتراک‌گذار اطلاعات	information sharing community	۸

ردیف	شماره بند	واژگان فارسی	واژگان انگلیسی	شماره صفحه
۳۹	۲-۳۹	سیستم اطلاعاتی	information system	۸
۴۰	۲-۴۰	یکپارچگی	integrity	۸
۴۱	۲-۴۱	طرف‌های علاقه‌مند	interested party	۸
۴۲	۲-۴۲	زمینهٔ درونی	internal context	۹
۴۳	۲-۴۳	پروژه ISMS	ISMS project	۹
۴۴	۲-۴۴	سطح مخاطره	level of risk	۹
۴۵	۲-۴۵	فرصت وقوع	likelihood	۹
۴۶	۲-۴۶	سیستم مدیریت	management system	۹
۴۷	۲-۴۷	سنجه	measure	۱۰
۴۸	۲-۴۸	سنجش	measurement	۱۰
۴۹	۲-۴۹	تابع سنجش	measurement function	۱۰
۵۰	۲-۵۰	روش سنجش	measurement method	۱۰
۵۱	۲-۵۱	نتایج سنجش	measurement results	۱۰
۵۲	۲-۵۲	پایش	monitoring	۱۱
۵۳	۲-۵۳	عدم انطباق	nonconformity	۱۱
۵۴	۲-۵۴	سلب انکار	non-repudiation	۱۱
۵۵	۲-۵۵	شیء	object	۱۱
۵۶	۲-۵۶	هدف	objective	۱۱
۵۷	۲-۵۷	سازمان	organization	۱۲
۵۸	۲-۵۸	برون‌سپاری کردن	outsource	۱۲
۵۹	۲-۵۹	عملکرد	performance	۱۲
۶۰	۲-۶۰	خط‌مشی	policy	۱۲
۶۱	۲-۶۱	فرآیند	process	۱۲

ردیف	شماره بند	واژگان فارسی	واژگان انگلیسی	شماره صفحه
۶۲	۲-۶۲	اطمینان پذیری	reliability	۱۳
۶۳	۲-۶۳	الزام	requirement	۱۳
۶۴	۲-۶۴	مخاطره باقیمانده	residual risk	۱۳
۶۵	۲-۶۵	بازنگری	review	۱۳
۶۶	۲-۶۶	شیء مورد بازنگری	review object	۱۳
۶۷	۲-۶۷	هدف بازنگری	review objective	۱۳
۶۸	۲-۶۸	مخاطره	risk	۱۴
۶۹	۲-۶۹	پذیرش مخاطره	risk acceptance	۱۴
۷۰	۲-۷۰	تحلیل مخاطره	risk analysis	۱۴
۷۱	۲-۷۱	ارزیابی مخاطره	risk assessment	۱۵
۷۲	۲-۷۲	اطلاع‌رسانی و مشاوره مخاطره	risk communication and consultation	۱۵
۷۳	۲-۷۳	معیار مخاطره	risk criteria	۱۵
۷۴	۲-۷۴	ارزشیابی مخاطره	risk evaluation	۱۵
۷۵	۲-۷۵	شناسایی مخاطره	risk identification	۱۵
۷۶	۲-۷۶	مدیریت مخاطره	risk management	۱۶
۷۷	۲-۷۷	فرآیند مدیریت مخاطره	risk management process	۱۶
۷۸	۲-۷۸	مالک مخاطره	risk owner	۱۶
۷۹	۲-۷۹	برطرف سازی مخاطره	risk treatment	۱۶
۸۰	۲-۸۰	مقیاس	scale	۱۷
۸۱	۲-۸۱	استاندارد پیاده‌سازی امنیت	security implementation standard	۱۷

ردیف	شماره بند	واژگان فارسی	واژگان انگلیسی	شماره صفحه
۸۲	۲-۸۲	ذینفع	stakeholder	۱۷
۸۳	۲-۸۳	تهدید	threat	۱۷
۸۴	۲-۸۴	مدیریت ارشد	top management	۱۸
۸۵	۲-۸۵	هستار قابل‌اعتماد تبادل اطلاعات	trusted information communication entity	۱۸
۸۶	۲-۸۶	واحد سنجش	unit of measurement	۱۸
۸۷	۲-۸۷	اعتبارسنجی	validation	۱۸
۸۸	۲-۸۸	درستی‌سنجی	verification	۱۸
۸۹	۲-۸۹	آسیب‌پذیری	vulnerability	۱۸

پیوست ت
(اطلاعاتی)
واژگان فارسی به انگلیسی

ردیف	واژه نامه فارسی (برحسب حروف الفبا)	واژگان انگلیسی
۱	آسیب‌پذیری	Vulnerability
۲	اتاق تجهیزات مخابراتی	Telecommunications equipment room
۳	اثربخشی	Effectiveness
۴	ارتباطات ضروری	Essential communications
۵	ارزش	Value
۶	ارزش اجتماعی	Societal value
۷	ارزش بازار	Market value
۸	ارزش تمدیدشده	Extended value
۹	ارزش در معرض مخاطره	Value-at-risk
۱۰	ارزش غیرمستقیم	Indirect value
۱۱	ارزش فرصت	Opportunity value
۱۲	ارزش فعلی	Present value
۱۳	ارزش فعلی خالص	Net present value
۱۴	ارزش مستقیم	direct value
۱۵	ارزش مورد انتظار	Expected value
۱۶	ارزش‌افزوده اقتصادی	Economic value added
۱۷	ارزشیابی مخاطره	Risk evaluation
۱۸	ارزیابی مخاطره	Risk assessment
۱۹	استاندارد پیاده‌سازی امنیت	Security implementation standard
۲۰	اصالت	Authenticity

ردیف	واژه نامه فارسی (برحسب حروف الفبا)	واژگان انگلیسی
۲۱	اصالت‌سنجی	Authentication
۲۲	اصلاح	Correction
۲۳	اطلاع‌رسانی و مشاوره مخاطره	Risk communication and consultation
۲۴	اطلاعات شخصی	Personalinformation
۲۵	اطلاعات مستند	Documented information
۲۶	اطمینان پذیری	Reliability
۲۷	اعتبارسنجی	Validation
۲۸	اقتصاد امنیت اطلاعات	Information security economics
۲۹	اقتصادی	Economics
۳۰	اقدام اصلاحی	Corrective action
۳۱	الزام	Requirement
۳۲	الزامات قراردادی	Regulatory requirements
۳۳	امنیت اطلاعات	Information security
۳۴	انطباق	Conformity
۳۵	بازنگری	Review
۳۶	باهم گذاری	Collocation
۳۷	برطرف سازی مخاطره	Risk treatment
۳۸	برون‌سپاری کردن	Outsource(verb)
۳۹	بهبود مستمر	Continual improvement
۴۰	پایش	Monitoring
۴۱	پذیرش مخاطره	Risk acceptance
۴۲	پروژه ISMS	ISMS project
۴۳	پیامد	Consequence

ردیف	واژه نامه فارسی (برحسب حروف الفبا)	واژگان انگلیسی
۴۴	تابع سنجش	Measurement function
۴۵	تحلیل مخاطره	Risk analysis
۴۶	تداوم امنیت اطلاعات	Information security continuity
۴۷	تسهیلات پایانه	Terminal facilities
۴۸	تسهیلات پردازش اطلاعات	Information processing facilities
۴۹	تسهیلات مخابراتی	Telecommunications facilities
۵۰	تماس اولویت‌دار	Perority call
۵۱	تهدید	Threat
۵۲	توجیه اقتصادی	Economic justification
۵۳	جامعه اشتراک‌گذار اطلاعات	Information sharing community
۵۴	حاکمیت امنیت اطلاعات	Governance of information security
۵۵	حمله	Attack
۵۶	خدمات مالی	Financial services
۵۷	خدمات مخابراتی	Telecommunications services
۵۸	خط‌مشی	Policy
۵۹	داده	Data
۶۰	درستی سنجی	Verification
۶۱	دسترس‌پذیری	Availability
۶۲	ذینفع	Stakeholder
۶۳	رخداد امنیت اطلاعات	Information security incident
۶۴	روش سنجش	Measurement method
۶۵	رویداد	Event
۶۶	رویداد امنیت اطلاعات	Information security event

ردیف	واژه نامه فارسی (برحسب حروف الفبا)	واژگان انگلیسی
۶۷	زمینه‌ی بیرونی	External context
۶۸	زمینه‌ی درونی	Internal context
۶۹	زیان	Loss
۷۰	زیان سالانه مورد انتظار	Annualized loss expectancy ALE
۷۱	سازمان	Organization
۷۲	سازمان	Organization
۷۳	سازمان‌های مخابراتی	Telecommunications organizations
۷۴	سطح مخاطره	Level of risk
۷۵	سلب انکار	Non-repudiation
۷۶	سنجش	Measurement
۷۷	سنجه	Measure
۷۸	سنجه مبنا	Base measure
۷۹	سنجه مشتق	Derived measure
۸۰	سند گواهی‌نامه	Certification document
۸۱	سوابق مخابراتی	Telecommunications records
۸۲	سیستم اطلاعاتی	Information system
۸۳	سیستم مدیریت	Management system
۸۴	شایستگی	Competence
۸۵	شناسایی مخاطره	Risk identification
۸۶	شیء	Object
۸۷	شیء موردبازنگری	Review object
۸۸	صفت	Attribute
۸۹	طرف‌علاقه‌مند	Interested party

ردیف	واژه نامه فارسی (برحسب حروف الفبا)	واژگان انگلیسی
۹۰	عامل اقتصادی	Economic factor
۹۱	عدم افشاء ارتباطات	Non-disclosure of communications
۹۲	عدم انطباق	Non-conformity
۹۳	علامت	Mark
۹۴	عملکرد	Performance
۹۵	فرآیند	Process
۹۶	فرآیند مدیریت مخاطره	Risk management process
۹۷	فرصت وقوع	Likelihood
۹۸	کاربر	User
۹۹	کاربر خدمت مخابراتی	Telecommunications service user
۱۰۰	کاربردهای مخابراتی	Telecommunications applications
۱۰۱	کسب‌وکار مخابراتی	Telecommunications business
۱۰۲	کنترل	Control
۱۰۳	کنترل دسترسی	Access control
۱۰۴	گواهی‌نامه	Certificate
۱۰۵	مالک مخاطره	Risk owner
۱۰۶	محدوده کاربرد ممیزی	Audit scope
۱۰۷	محرمانگی	Confidentiality
۱۰۸	مخاطره	Risk
۱۰۹	مخاطره باقیمانده	Residual risk
۱۱۰	مدل تحلیلی	Analytical model
۱۱۱	مدیریت اجرایی	Executive management
۱۱۲	مدیریت ارشد	Top management

ردیف	واژه نامه فارسی (برحسب حروف الفبا)	واژگان انگلیسی
۱۱۳	مدیریت امنیت اطلاعات	Information security management IMS
۱۱۴	مدیریت رخداد امنیت اطلاعات	Information security incident management
۱۱۵	مدیریت مخاطره	Risk management
۱۱۶	مرکز ارتباط	Communication centre
۱۱۷	مزیت غیراقتصادی	Non economic benefit
۱۱۸	مشتری خدمت مخابراتی	Telecommunications service customer
۱۱۹	معیار تصمیم‌گیری	Decision criteria
۱۲۰	معیار مخاطره	Risk criteria
۱۲۱	مقایسه اقتصادی	Economic comparison
۱۲۲	مقیاس	Scale
۱۲۳	ممیزی	Audit
۱۲۴	نتایج سنجش	Measurement results
۱۲۵	نرخ بازگشت سرمایه	Return on investment
۱۲۶	نشانگر	Indicator
۱۲۷	نهاد حکومتی	Governing body
۱۲۸	نهاد صدور گواهی	Certification body
۱۲۹	نیاز اطلاعاتی	Information need
۱۳۰	واحد سنجش	Unit of measurement
۱۳۱	هدف	Objective
۱۳۲	هدف بازنگری	Review objective
۱۳۳	هدف کنترلی	Control objective
۱۳۴	هزینه فرصت	Opportunity cost
۱۳۵	هستار مورد اعتماد ارتباط اطلاعات	Trusted information communication entity

ردیف	واژه نامه فارسی (برحسب حروف الفبا)	واژگان انگلیسی
۱۳۶	یکپارچگی	Integrity

پیوست ث
(اطلاعاتی)
واژگان انگلیسی به فارسی

ردیف	واژگان انگلیسی	واژه نامه فارسی
1	Access control	کنترل دسترسی
2	Analytical model	مدل تحلیلی
3	Annualized loss expectancy ALE	زیان سالانه مورد انتظار
4	Attack	حمله
5	Attribute	صفت
6	Audit	ممیزی
7	Audit scope	محدوده کاربرد ممیزی
8	Authentication	اصالت‌سنجی
9	Authenticity	اصالت
10	Availability	دسترس‌پذیری
11	Base measure	سنجه مبنا
12	Certificate	گواهی‌نامه
13	Certification body	نهاد صدور گواهی
14	Certification document	سند گواهی‌نامه
15	Collocation	باهم گذاری
16	Communication centre	مرکز ارتباط
17	Competence	شایستگی
18	Confidentiality	محرمانگی
19	Conformity	انطباق
20	Consequence	پیامد
21	Continual improvement	بهبود مستمر

ردیف	واژگان انگلیسی	واژه نامه فارسی
22	Control	کنترل
23	Control objective	هدف کنترلی
24	Correction	اصلاح
25	Corrective action	اقدام اصلاحی
26	Data	داده
27	Decision criteria	معیار تصمیم‌گیری
28	Derived measure	سنجه مشتق
29	direct value	ارزش مستقیم
30	Documented information	اطلاعات مستند
31	Economic comparison	مقایسه اقتصادی
32	Economic factor	عامل اقتصادی
33	Economic justification	توجیه اقتصادی
34	Economic value added	ارزش‌افزوده اقتصادی
35	Economics	اقتصادی
36	Effectiveness	اثربخشی
37	Essential communications	ارتباطات ضروری
38	Event	رویداد
39	Executive management	مدیریت اجرایی
40	Expected value	ارزش مورد انتظار
41	Extended value	ارزش تمدیدشده
42	External context	زمینه‌ی بیرونی
43	Financial services	خدمات مالی
44	Governance of information security	حاکمیت امنیت اطلاعات
45	Governing body	نهاد حکومتی

ردیف	واژگان انگلیسی	واژه نامه فارسی
46	Indicator	نشانگر
47	Indirect value	ارزش غیرمستقیم
48	Information need	نیاز اطلاعاتی
49	Information processing facilities	تسهیلات پردازش اطلاعات
50	Information security	امنیت اطلاعات
51	Information security continuity	تداوم امنیت اطلاعات
52	Information security economics	اقتصاد امنیت اطلاعات
53	Information security event	رویداد امنیت اطلاعات
54	Information security incident	رخداد امنیت اطلاعات
55	Information security incident management	مدیریت رخداد امنیت اطلاعات
56	Information security management IMS	مدیریت امنیت اطلاعات
57	Information sharing community	جامعه اشتراک‌گذار اطلاعات
58	Information system	سیستم اطلاعاتی
59	Integrity	یکپارچگی
60	Interested party	طرف‌علاقه‌مند
61	Internal context	زمینه‌ی درونی
62	ISMS project	پروژه ISMS
63	Level of risk	سطح مخاطره
64	Likelihood	فرصت وقوع
65	Loss	زیان
66	Management system	سیستم مدیریت
67	Mark	علامت
68	Market value	ارزش بازار
69	Measure	سنجه

ردیف	واژگان انگلیسی	واژه نامه فارسی
70	Measurement	سنجش
71	Measurement function	تابع سنجش
72	Measurement method	روش سنجش
73	Measurement results	نتایج سنجش
74	Monitoring	پایش
75	Net present value	ارزش فعلی خالص
76	Non economic benefit	مزیت غیراقتصادی
77	Non-conformity	عدم انطباق
78	Non-disclosure of communications	عدم افشاء ارتباطات
79	Non-repudiation	سلب انکار
80	Object	شیء
81	Objective	هدف
82	Opportunity cost	هزینه فرصت
83	Opportunity value	ارزش فرصت
84	Organization	سازمان
85	Organization	سازمان
86	Outsource(verb)	برون‌سپاری کردن
87	Performance	عملکرد
88	Perority call	تماس اولویت‌دار
89	Personalinformation	اطلاعات شخصی
90	Policy	خط‌مشی
91	Present value	ارزش فعلی
92	Process	فرآیند
93	Regulatory requirements	الزامات قراردادی

ردیف	واژگان انگلیسی	واژه نامه فارسی
94	Reliability	اطمینان پذیری
95	Requirement	الزام
96	Residual risk	مخاطره باقیمانده
97	Return on investment	نرخ بازگشت سرمایه
98	Review	بازنگری
99	Review object	شیء موردبازنگری
100	Review objective	هدف بازنگری
101	Risk	مخاطره
102	Risk acceptance	پذیرش مخاطره
103	Risk analysis	تحلیل مخاطره
104	Risk assessment	ارزیابی مخاطره
105	Risk communication and consultation	اطلاع‌رسانی و مشاوره مخاطره
106	Risk criteria	معیار مخاطره
107	Risk evaluation	ارزشیابی مخاطره
108	Risk identification	شناسایی مخاطره
109	Risk management	مدیریت مخاطره
110	Risk management process	فرآیند مدیریت مخاطره
111	Risk owner	مالک مخاطره
112	Risk treatment	برطرف سازی مخاطره
113	Scale	مقیاس
114	Security implementation standard	استاندارد پیاده‌سازی امنیت
115	Societal value	ارزش اجتماعی
116	Stakeholder	ذینفع
117	Telecommunications applications	کاربردهای مخابراتی

ردیف	واژگان انگلیسی	واژه نامه فارسی
118	Telecommunications business	کسب‌وکار مخابراتی
119	Telecommunications equipment room	اتاق تجهیزات مخابراتی
120	Telecommunications facilities	تسهیلات مخابراتی
121	Telecommunications organizations	سازمان‌های مخابراتی
122	Telecommunications records	سوابق مخابراتی
123	Telecommunications service customer	مشتری خدمت مخابراتی
124	Telecommunications service user	کاربر خدمت مخابراتی
125	Telecommunications services	خدمات مخابراتی
126	Terminal facilities	تسهیلات پایانه
127	Threat	تهدید
128	Top management	مدیریت ارشد
129	Trusted information communication entity	هستار مورد اعتماد ارتباط اطلاعات
130	Unit of measurement	واحد سنجش
131	User	کاربر
132	Validation	اعتبارسنجی
133	Value	ارزش
134	Value-at-risk	ارزش در معرض مخاطره
135	Verification	درستی سنجی
136	Vulnerability	آسیب‌پذیری

کتاب‌نامه

[1] ISO/IEC 17021:2011, Conformity assessment — Requirements for bodies providing audit and certification of management systems

[2] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary

[3] ISO 19011:2011, Guidelines for auditing management systems

[4] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[5] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[6] ISO/IEC 27003:2010, Information technology — Security techniques — Information security management system implementation guidance

[7] ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement

[8] ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management

[9] ISO/IEC 27006:2011, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[10] ISO/IEC 27007:2011, Information technology — Security techniques — Guidelines for informationsecurity management systems auditing

[11] ISO/IEC TR 27008:2011, Information technology — Security techniques — Guidelines for auditorson information security controls

[12] ISO/IEC 27010:2012, Information technology — Security techniques — Information securitymanagement for inter-sector and inter-organizational communications

[13] ISO/IEC 27011:2008, Information technology — Security techniques — Information securitymanagement guidelines for telecommunications organizations based on ISO/IEC 27002

[14] ISO/IEC 27013:2012, Information technology — Security techniques — Guidance on the integratedimplementation of ISO/IEC 27001 and ISO/IEC 20000-1

[15] ISO/IEC 27014:2013, Information technology — Security techniques — Governance of informationsecurity

[16] ISO/IEC TR 27015:2012, Information technology — Security techniques — Information securitymanagement guidelines for financial services

[17] ISO/IEC TR 27016-2, Information technology — Security techniques — Information securitymanagement — Organizational economics

[18] ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC27002

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

[20] ISO/IEC 15939:2007, Systems and software engineering — Measurement process

[21] ISO/IEC 20000-1, Information technology — Service management — Part 1: Service managementsystemrequirements