

INSO-ISO-IEC

27000

1st.Revision

2015



جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization



استاندارد ملی ایران - ایزو -

آی ای سی

۲۷۰۰۰

تجدیدنظر اول

۱۳۹۴

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

مؤسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه 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 و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف کنندگان، 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 می شود و پس از دریافت نظرها و پیشنهادات در کمیته 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 در کمیته ملی طرح و بررسی و در صورت 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 شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)^۱، کمیسیون بین المللی الکتروتکنیک (IEC)^۲ و سازمان بین المللی اندازه شناسی قانونی (OIML)^۳ است و به عنوان تنها رابط^۴ کمیسیون کدکس غذایی (CAC)^۵ 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 بین المللی بهره گیری می شود.

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 استانداردهای کالاهای صادراتی و درجه بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) و 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، گواهینامه تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) و وسایل سنجش، تعیین عبار 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 (سیستم های) مدیریت امنیت اطلاعات - مرور کلی
وواژگان»

رئیس:

مرتضوی، محمود
(دکتر مهندسی نرم افزار)

سمت و / یا نمایندگی:

مدیر فنی 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)

ایزدینا، 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

معاون مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران	کیامهر، بیتا (کارشناسی ارشد مدیریت تکنولوژی)
کارشناس رسمی دادگستری	محمودی، یعقوب (کارشناسی ارشد فناوری اطلاعات، سیستم‌های اطلاعاتی)
کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران	مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)
رئیس هیأت مدیره شرکت داده پردازان آبشار	مهدوی اردستانی، علیرضا (کارشناسی ارشد مدیریت فناوری اطلاعات، سیستم- های اطلاعاتی پیشرفته)
مدیرعامل پژوهش های راهبردی امن رای	میرمعینی، علیرضا (کارشناسی ارشد مهندسی صنایع،)

فهرست مندرجات

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

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

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی-سامانه های (سیستم‌های) مدیریت امنیت اطلاعات- مرور کلی 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 زیر است:

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.

استانداردهای ملی سیستم‌های مدیریت، به منظور فراهم آوردن مدلی برای استقرار و بهره‌برداری^۱ از سیستم مدیریت تهیه شده 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 27^۲، شامل گروهی تخصصی است که به تدوین استانداردهای سیستم‌های مدیریت بین‌المللی امنیت اطلاعات می‌پردازد. این استانداردها به‌عنوان استانداردهای خانواده سیستم مدیریت امنیت اطلاعات (ISMS)^۳ شناخته می‌شوند.

سازمان‌ها می‌توانند با استفاده از استانداردهای خانواده ISMS، چارچوبی را برای مدیریت امنیت دارایی‌های اطلاعاتی خود شامل اطلاعات مالی^۴، مالکیت معنوی^۵، جزئیات اطلاعات کارکنان^۶ یا اطلاعات سپرده شده به آن‌ها توسط مشتریان یا طرف‌های سوم^۷ تدوین و پیاده‌سازی کنند. این استانداردها می‌توانند برای ارزیابی^۸ مستقل سیستم مدیریت امنیت اطلاعات سازمان‌ها، به منظور حفاظت از اطلاعات به کار گرفته شوند.

۲-۰ استانداردهای خانواده ISMS

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

- ISO/IEC 27000^۹، سیستم‌های مدیریت امنیت اطلاعات - مرور کلی و واژگان
- ISO/IEC 27001^{۱۰}، سیستم‌های مدیریت امنیت اطلاعات - الزامات
- ISO/IEC 27002^{۱۱}، آیین کار کنترل^{۱۲}های امنیت اطلاعات
- ISO/IEC 27003^۱، 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 ۱۳۸۷ با 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 ارائه‌دهنده 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.

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^۱ موسوم به فناوری اطلاعات، تدوین شده است. استانداردهای بین‌المللی که تحت همین عنوان عمومی نیستند و درعین حال قسمتی از استانداردهای خانواده ISMS محسوب می‌شوند، عبارتند از:

– ISO 27799:2008^۲، انفورماتیک سلامت- مدیریت امنیت اطلاعات در بهداشت با استفاده از ISO/IEC 27002

۳-۰ هدف از این استاندارد ملی

این استاندارد ملی، مرور کلی 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 مشخص شده 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^۴ ISMS می‌پردازد.

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

- اصطلاحات و تعاریف متداول در خانواده استانداردهای ISMS را در برمی‌گیرد؛
- تمام اصطلاحات و تعاریف به کارگرفته شده در استانداردهای خانواده ISMS را در برنمی‌گیرد؛ 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 ISIRI ۱۳۲۲۰ در سال ۱۳۸۹ با منبع بین‌المللی ISO 27799:2008 انفورماتیک سلامت، منتشر شده است.

4 - Conformity Assessment

فناوری اطلاعات - فنون امنیتی - سامانه های (سیستم های) مدیریت امنیت

اطلاعات - مرور کلی و واژگان

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و راهنمایی برای مرور کلی بر سیستم های مدیریت امنیت اطلاعات و اصطلاحات و تعاریف که به صورت عمومی مورد استفاده در خانواده استانداردهای ISMS است. این استاندارد در تمامی انواع سازمان ها در هر اندازه ای^۱ کاربردپذیر است (مانند بنگاه های تجاری^۲، دستگاه های دولتی^۳، سازمان های غیرانتفاعی^۴).

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

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می رود:

۱-۲

کنترل دسترسی

حصول اطمینان از اینکه دسترسی به دارایی ها به صورت مجاز و محدود بر اساس الزامات امنیتی و الزامات کسب و کار است.

۲-۲

مدل تحلیلی

الگوریتم یا محاسبه ای که یک یا چندین سنجه مبنا^۵ (۲-۱۰) و/یا سنجه های مشتق^۶ (۲-۲۲) را با معیار تصمیم گیری^۷ مرتبط، ترکیب می کند.

۳-۲

حمله

تلاشی جهت تخریب، افشا، دست کاری، 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 مشخصه شی (۲-۵۵) که به صورت کیفی یا کمی توسط انسان یا ابزارهای خودکار^۱ قابل تشخیص است.

[منبع: استاندارد ملی ایران شماره ۱۲۷۵۵: سال ۱۳۸۷، تغییر یافته - 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، به منظور 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

اصالت سنجی

کسب اطمینان از آنکه مشخصه ادعا شده هستار، درست است.

۸-۲

اصالت

خصوصیتی که یک هستار، همان است که ادعا می‌کند.

۹-۲

دسترس پذیری

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

۱۰-۲

سنجه مينا

سنجه‌ای (۴۷-۲) است که برحسب یک صفت (۴-۲) و روش کمی کردن آن تعریف شده است.

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

یادآوری ۱- هر سنجه مینا، از لحاظ کارکردی، مستقل از سایر سنجه‌ها است.

۱۱-۲

شایستگی

توانایی به کارگیری دانش و مهارت‌ها جهت رسیدن به نتایج موردنظر است.

۱۲-۲

محرمانگی

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

۱۳-۲

انطباق

تحقق یک الزام (۶۳-۲) است.

یادآوری ۱- اصطلاح «متابعت^۱» مترادف است ولی مناسب نیست^۲.

۱۴-۲

پیامد

خروجی یک رویداد (۲۵-۲) که بر اهداف (۵۶-۲) 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 زمینه امنیت اطلاعات، منفی است.

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

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

۱۵-۲

بهبود مستمر

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

1- Conformance

۲- در متن انگلیسی این متن آمده است ولی در متن فارسی می‌توان 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 نتیجه پیاده‌سازی کنترل‌ها (۲-۱۶) به دست آید را توصیف می‌کند.

۱۸-۲

اصلاح

اقدامی که برای از بین بردن عدم انطباق (۲-۵۳) شناسایی شده 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 داده شده است.

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

یادآوری ۱- این تعریف فقط در زمینه 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 ارائه شده توصیف می‌شود.

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

۲۲-۲

سنجه مشتق

سنجه‌ای (۲-۴۷) است که به صورت تابعی از مقادیر دو یا چند سنجه مبنا (۲-۱۰) تعریف شده 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 تأمین شده باشد.

یادآوری ۲- اطلاعات مستند می‌تواند اشاره داشته باشد به:

- سیستم مدیریت (۲-۴۶)، شامل فرآیندهای (۲-۶۱) مرتبط؛
- اطلاعات ایجاد شده جهت عملیات سازمان (مستندسازی)؛
- شواهد نتایج به دست آمده (سوابق).

۲۴-۲

اثر بخشی

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

۲۵-۲

رویداد

وقوع یا تغییر مجموعه‌ای ویژه از شرایط است.

[منبع: ISO Guide73:2009]

یادآوری ۱- رویداد^۱ می‌تواند یک یا چندین اتفاق^۲ 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^۳» یا «حادثه^۴» 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^۱ (۲۹-۲) برای پیاده‌سازی راهبردها و خط‌مشی‌ها جهت تحقق اهداف سازمان (۵۷-۲) دارای اختیار هستند.

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

۲۷-۲

زمینه بیرونی

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

[منبع: ISO Guide73:2009]

یادآوری ۱- زمینه بیرونی می‌تواند شامل موارد زیر باشد:

- محیط فرهنگی، اجتماعی، سیاسی، قانونی^۲، مقررات تنظیمی^۳، فناوریانه، اقتصادی، طبیعی، رقابتی، به‌صورت بین-المللی، ملی، منطقه‌ای یا محلی؛
- پیشران‌ها و روندهای کلیدی تأثیرگذار بر اهداف (۵۶-۲) سازمان (۵۷-۲)؛ و
- ارتباطات، ادراکات^۴ و ارزش‌های ذی‌نفعان (۸۲-۲) بیرونی؛

۲۸-۲

حاکمیت امنیت اطلاعات

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

۲۹-۲

هیأت حاکم

فرد یا گروهی از افراد که پاسخگوی انطباق و عملکرد (۵۹-۲) سازمان (۵۷-۲) 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 (۴۷-۲) است جهت تخمین یا ارزشیابی صفات (۴-۲) مشخص که با توجه به نیازهای اطلاعاتی (۲-۲) (۳۱) تعریف شده 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 (۱۲-۲)، یکپارچگی (۴۰-۲) و دسترس پذیری (۹-۲) اطلاعات است.

یادآوری ۱- علاوه بر این، سایر خصوصیت‌ها، همچون اصالت (۸-۲)، پاسخگویی، سلب انکار (۵۴-۲) و اطمینان پذیری (۶۲-۲) را نیز می‌تواند دربرگیرد.

۳۴-۲

تداوم امنیت اطلاعات

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

۳۵-۲

رویداد امنیت اطلاعات

وقوع یک حالت شناخته شده 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 (۳۵-۲) ناخواسته یا پیش‌بینی نشده که به احتمال زیاد عملیات کسب‌وکار را به خطر می‌اندازد و امنیت اطلاعات (۳۳-۲) را تهدید می‌کند.

۳۷-۲

مدیریت رخدادهای امنیت اطلاعات

فرآیندهایی (۲-۶۱) به منظور آشکارسازی، گزارش دهی، ارزیابی، پاسخ‌دهی به، رسیدگی به و یادگیری 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^۱ 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 یا خود را متأثر از آن بداند.

۴۲-۲

زمینه 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؛

- ظرفیت‌ها که به صورت منابع و دانش (به‌عنوان مثال: سرمایه، زمان، افراد، فرآیندها، سیستم‌ها، فناوری‌ها) درک شده است؛
- سامانه‌های اطلاعاتی، جریان‌های اطلاعاتی و فرآیندهای تصمیم‌سازی (به صورت 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 ساختارمند که سازمان (۲-۵۷) جهت پیاده‌سازی ISMS انجام می‌دهد.

۴۴-۲

سطح مخاطره

شدت مخاطره (۲-۶۸) که به صورت ترکیبی از پیامدها (۲-۱۴) و فرصت وقوع^۱ (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)، اهداف (۲-۵۶) و فرآیندها (۲-۶۱) به منظور دستیابی به اهداف سازمان است.

یادآوری ۱- سیستم مدیریت می‌تواند به یک یا چندین نظام مدیریتی^۲ 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، بخش‌های مشخص و تعیین‌شده سازمان یا یک یا چندین کارکرد بین، گروهی از سازمان‌ها باشد.

1 -likelihood

2- Discipline

۴۷-۲

سنجه

متغیری که به واسطه نتیجه سنجش (۲-۴۸) مقداری به آن نسبت داده شده است.

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

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

۴۸-۲

سنجش

فرآیند (۲-۶۱) تعیین ارزش است.

یادآوری ۱- درزمینه 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 چندسنجه مبنا (۲-۱۰) انجام می‌شود.

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

۵۰-۲

روش سنجش

ترتیب منطقی کارها که به صورت عام تعریف شده است و برای کمی 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 کمی سازی یک صفت مورد استفاده قرار گرفته است. دو نوع روش قابل تمایز است:

- ذهنی: کمی سازی که در آن قضاوت انسان نقش دارد.

- عینی: کمی 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 (۶۱-۲) 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 (۶۳-۲) است.

۵۴-۲

سلب انکار

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

۵۵-۲

شیء

عنصری که به واسطهٔ سنجش (۴۸-۲) صفت‌هایش (۴-۲) مشخص شده است.

۵۶-۲

هدف

نتیجه‌ای که باید به دست آید.

یادآوری ۱- هدف می‌تواند راهبردی، راه‌کنشی^۱ 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 (۶۱-۲)).

یادآوری ۳- هدف می‌تواند به اشکال دیگری مانند دستاورد موردنظر، هدف، معیار عملکردی، 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 تعیین شده و با خط‌مشی امنیت اطلاعات سازگار می‌شوند تا نتایج موردنظر به دست آید.

^۱ tactical

۵۷-۲

سازمان

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

یادآوری ۱- مفهوم سازمان، کسب‌وکار فردی، شرکت تجاری، شرکت سهامی، موسسه بازرگانی، تشکیلات اقتصادی، نمایندگی مجاز، مشارکت، خیریه و مؤسسات، یا قسمتی یا ترکیبی از اینها، خواه با هم همکاری کنند یا خیر، خصوصی باشند یا عمومی باشند را شامل می‌شود اما محدود به اینها نیست.

۵۸-۲

برون‌سپاری کردن

ترتیب دادن امور به گونه‌ای 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 برون‌سپاری شده، درون محدوده باشد.

۵۹-۲

عملکرد

نتیجه قابل اندازه‌گیری است.

یادآوری ۱- عملکرد می‌تواند به یافته‌های کیفی یا کمی 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

خواست‌ها و جهت‌گیری سازمان (۲-۵۷) که توسط مدیریت ارشد (۲-۸۴) به صورت رسمی بیان شده است.

۶۱-۲

فرآیند

مجموعه‌ای از فعالیت‌های مرتبط و متعامل که ورودی‌ها^۱ را به خروجی‌ها^۲ 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 تصریح شده، به صورت عام دلالت ضمنی دارد، یا دارای اجبار قانونی است.

یادآوری ۱- «به صورت عام دلالت ضمنی داشته» به این معنی است که آن نیاز یا انتظار مورد نظر به صورت ضمنی، اقدامی متداول و مرسوم برای سازمان و طرفهای علاقه مند محسوب می شود.

یادآوری ۲- الزام مشخص شده، الزامی است که تصریح شده است به عنوان مثال در اطلاعات مستند.

۶۴-۲

مخاطره باقیمانده

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

یادآوری ۱- مخاطره باقیمانده می تواند شامل مخاطره شناسایی نشده باشد.

یادآوری ۲- مخاطره باقیمانده تحت عنوان «مخاطرات نگه داشته شده^۱» نیز شناخته می شود.

۶۵-۲

بازنگری

فعالیتی است که جهت تعیین میزان تناسب، کفایت و اثربخشی (۲۴-۲) یک موضوع به منظور دستیابی به اهداف مقرر شده انجام می شود.

[منبع: ISO Guide 73:2009]

۶۶-۲

شیء مورد بازنگری

عنصر^۲ مشخصی که مورد بازنگری قرار می گیرد.

۶۷-۲

هدف بازنگری

بیانهای که آنچه باید از نتیجه بازنگری به دست آید را توصیف می کند.

1- Retained risk

2- Item

۶۸-۲

مخاطره

اثر عدم قطعیت^۱ 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 به رویداد (۲-۲) (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 می شود.

یادآوری ۴- مخاطره معمولاً به صورت ترکیبی از پیامدهای (۲-۱۴) یک رویداد (شامل تغییر شرایط) و فرصت وقوع (۲-۴۵) مرتبط با آن بیان می شود.

یادآوری ۵- در زمینه سیستم های مدیریت امنیت اطلاعات، مخاطرات امنیت اطلاعات می تواند به صورت تأثیر عدم قطعیت بر اهداف امنیت اطلاعات بیان شود.

یادآوری ۶- مخاطره امنیت اطلاعات با پتانسیل بهره جویی تهدیدات (۲-۸۳) از آسیب پذیری های (۲-۸۹) یک دارایی اطلاعاتی یا گروهی از آنها و آسیب رسانی 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 می تواند بدون برطرف سازی (۲-۷۹) مخاطره یا طی فرآیند برطرف سازی مخاطره انجام شود.

یادآوری ۲- مخاطرات پذیرفته شده مورد پایش (۲-۵۲) و بازنگری (۲-۶۵) قرار می گیرند.

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 برطرف سازی مخاطره (۲-۷۹) فراهم می کند.

یادآوری ۲- تحلیل مخاطره شامل تخمین مخاطره است.

1- Uncertainty

۷۱-۲

ارزیابی مخاطره

فرآیند (۶۱-۲) کلان شناسایی (۷۵-۲)، تحلیل (۷۰-۲) و ارزشیابی مخاطره (۷۴-۲) 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 (۸۲-۲) در ارتباط با مدیریت مخاطره (۶۸-۲) 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 نمی‌آید.

۷۳-۲

معیار مخاطره

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

[منبع: ISO Guide73:2009]

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

۷۵-۲

شناسایی مخاطره

فرآیند یافتن، تشخیص و توصیف مخاطرات (۶۸-۲) 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 کلی مدیریت مخاطره به کار می‌برد. عناصر درون فرآیند مدیریت مخاطره اصطلاحاً «فعالیت» نامیده می‌شود.

۷۸-۲

مالک مخاطره

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

[منبع: ISO Guide73:2009]

۷۹-۲

برطرف‌سازی 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 فعالیت‌هایی که مخاطره را افزایش می‌دهد؛
- پذیرش یا افزایش مخاطره به‌منظور فرصت‌سازی؛
- 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- برطرف‌سازی مخاطره می‌تواند منجر به ایجاد مخاطرات جدید یا تغییر مخاطرات موجود شود.

۸۰-۲

مقیاس

مجموعه‌ی 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 رده‌بندی شده 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 عهده دارند.

یادآوری ۱- مدیریت ارشد قدرت تفویض اختیار و فراهم سازی 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 می کنند.

۸۵-۲

هستار قابل اعتماد تبادل اطلاعات

سازمان مستقلی که مبادله اطلاعات در جامعه اشتراک گذاران اطلاعات را حمایت می کند.

۸۶-۲

واحد سنجش

کمیتی مشخص که طبق توافقی تعریف و پذیرفته شده است و به کمک آن کمیت، اندازه سایر کمیت های هم نوع نسبت به آن با یکدیگر مقایسه می شوند.

[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

درستی سنجی

تائیدی است بر اساس تهیه شواهد عینی، مبنی بر اینکه الزامات مشخص شده برآورده شده است.

[منبع: : استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

یادآوری ۱- همچنین می تواند آزمون انطباق نامیده شود.

۸۹-۲

آسیب پذیری

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

سیستم‌های مدیریت امنیت اطلاعات ۳

۱-۳ 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 غیرقابل قبول 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 مرور کلی 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 به صورت تجمیعی مدیریت می‌شود. سیستم مدیریت امنیت اطلاعات یک رویکرد نظام‌مند برای استقرار، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات یک سازمان به منظور تحقق اهداف کسب‌وکار فراهم می‌سازد که مبتنی بر ارزیابی مخاطره و سطوح قابل قبول مخاطره سازمان برای برطرف‌سازی و مدیریت مؤثر مخاطرات طراحی شده است. تحلیل الزامات به منظور 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 به ضرورت 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 قابل قبول مخاطره؛

ج- در نظر گرفتن امنیت به عنوان 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 در نتیجه نیاز به حفاظت مناسب دارد. اطلاعات را می‌توان به شکل‌های بسیاری ذخیره کرد، از جمله: به شکل دیجیتالی (برای مثال داده‌های ذخیره‌شده در رسانه نوری یا الکترونیکی)، به شکل فیزیکی (برای مثال بر روی کاغذ) و همچنین اطلاعات نامشهود مانند دانش کارکنان. اطلاعات را می‌توان با روش‌های مختلفی برای مثال با استفاده از پیک، ارتباطات الکترونیکی یا به صورت شفاهی انتقال داد. اطلاعات، به هر شکلی که باشد، یا با هر روشی که انتقال یابد، همیشه به حفاظت مناسب نیاز دارد.

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، دسترس پذیری و یکپارچگی. امنیت اطلاعات شامل به کارگیری و مدیریت معیارهای امنیتی مناسبی است که بازه گسترده‌ای از تهدیدات را مورد توجه قرار می‌دهد و به دنبال اطمینان از موفقیت پایدار و تداوم کسب و کار 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، انتخاب شده و با استفاده از ISMS مدیریت می‌شود که شامل خط‌مشی‌ها، فرآیندها، روش‌های اجرایی، ساختارهای سازمانی، نرم‌افزارها و سخت‌افزارها به منظور حفاظت از دارایی‌های اطلاعاتی شناسایی شده است. به منظور اطمینان از دستیابی به اهداف امنیت اطلاعات و کسب و کار سازمان، این کنترل‌ها باید تعیین، پیاده‌سازی، پایش، بازنگری و در صورت نیاز بهبود داده شوند. کنترل‌های مرتبط با امنیت اطلاعات باید به صورت تنگاتنگی با فرآیندهای کسب و کار سازمان یکپارچه شده باشند.

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 دیدگاه ISMS، مدیریت عبارت از نظارت و تصمیم‌گیری‌های لازم برای رسیدن به اهداف کسب و کار 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^۱ 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 از لحاظ امنیت اطلاعات، سازمان را قادر می‌سازد تا:

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

ب- فعالیت‌ها و طرح‌های سازمان را بهبود دهد؛

پ- اهداف امنیت اطلاعات سازمان را محقق سازد؛

1- Individual associated

ت- با مقررات، قوانین والزامات^۱ صنفی تطبیق یابد؛ و

ث- دارایی‌های اطلاعاتی را به صورت سازمان یافته‌ای مدیریت کند به طوری که بهبود مستمر وسازگاری با اهداف کنونی سازمان تسهیل شود.

۳-۳ رویکرد فرآیندی^۲

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 به کارگیری مجموعه‌ای از فعالیت‌های مرتبط و متعامل که یک فرآیند نیز نامیده می‌شود، ممکن سازد. ورودی یک فرآیند می‌تواند به طور مستقیم ورودی فرآیند دیگری باشد و عموماً این تبدیل در شرایط کنترل شده و برنامه ریزی شده صورت می‌گیرد. به کارگیری سیستمی از فرآیندها در یک سازمان، همراه با شناسایی و تعامل این فرآیندها و مدیریت آن‌ها را می‌توان «رویکرد فرآیندی» نامید.

۴-۳ چرا ISMS مهم است؟

مخاطرات مرتبط با دارایی‌های اطلاعاتی سازمان باید مورد توجه قرار گیرند. رسیدن به امنیت اطلاعات به مدیریت مخاطره نیاز دارد و شامل مخاطرات ناشی از تهدیدهای فیزیکی، انسانی و فناوری مرتبط با تمام اشکال اطلاعات درون سازمانی و مورد استفاده سازمان می‌شوند.

انتظار می‌رود پذیرش ISMS، تصمیمی راهبردی برای سازمان باشد و لازم است این تصمیم بر طبق نیازهای سازمان، کاملاً یکپارچه، متناسب^۳ و به روز شود.

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

در دنیای به هم پیوسته^۴، اطلاعات و فرآیندها، سیستم‌ها و شبکه‌های مرتبط، دارایی‌های حیاتی کسب و کار را تشکیل می‌دهند. سازمان‌ها و سیستم‌ها و شبکه‌های اطلاعاتی آن‌ها، با تهدیدهای امنیتی از سوی گستره‌ی وسیعی از منابع شامل تقلب رایانه‌ای^۵، جاسوسی^۶، خرابکاری^۷، تخریب^۸، آتش‌سوزی و سیل روبرو می‌شوند.

1 - Mandates

2 - Process Approach

3 - Scaled

4 - Interconnected World

5 - Computer assisted 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)^۱، بیش از پیش فراگیر، جاه‌طلبانه‌تر و به‌طور فزاینده‌ای پیچیده شده است.

ISMS برای کسب‌وکارهای هر دو بخش عمومی و خصوصی مهم است. در هر صنعتی، ISMS، عاملی توانمندساز^۲ 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.

در بسیاری 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 در سیستم 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 بر الزامات 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 کاربردی‌پذیر 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

۵-۳ استقرار، پایش، نگهداری و بهبود ISMS

۱-۵-۳ مرور کلی

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

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

ب- 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 غیرقابل پذیرش (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 مستمر ISMS از دارایی‌های اطلاعاتی سازمان، لازم است مراحل «الف» تا «ت» به‌طور مداوم جهت شناسایی تغییر در مخاطرات یا در راهبردهای سازمان یا اهداف کسب و کار تکرار شود.

۲-۵-۳ شناسایی الزامات امنیت اطلاعات

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

الف- دارایی‌های اطلاعاتی شناسایی شده و ارزش آنها؛

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

پ- الزامات قانونی، مقررات تنظیم‌شده و قراردادی.

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 و کار 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، کمی‌سازی و اولویت‌بندی 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 پیاده‌سازی کنترل‌های 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 زده شده با معیارهای مخاطره داشته باشد تا میزان اهمیت مخاطرات مشخص شود (ارزشیابی مخاطره).

توصیه می‌شود ارزیابی‌های مخاطره به صورت 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 مناسب بودن، 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 فراهم شده است. مثال‌هایی از روشگان^۱ ارزیابی مخاطره نیز لحاظ شده است.

۳-۵-۴ برطرف‌سازی مخاطرات امنیت اطلاعات

توصیه می‌شود، سازمان قبل از برطرف‌سازی مخاطره، در مورد معیارهایی که بر اساس آن تعیین می‌کند مخاطرات قابل پذیرش هستند یا خیر، تصمیم‌گیری کند. مخاطرات ممکن است مورد پذیرش قرار گیرند، اگر به عنوان مثال مخاطره پائین ارزیابی شده باشد یا اینکه هزینه برطرف‌سازی مخاطرات مقرون به صرفه نباشد. توصیه می‌شود این تصمیم‌ها، ثبت شده باشد.

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

الف- به کارگیری کنترل‌های مناسب جهت کاهش مخاطرات؛

ب- پذیرش آگاهانه و هدفمند مخاطرات مشروط بر اینکه به وضوح، 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).

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

۳-۵-۵ انتخاب و پیاده‌سازی کنترل‌ها

به محض این که 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 پیاده‌سازی کنترل‌ها 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 کاهش یافته و مخاطرات باقیمانده به نسبت محدودیت‌ها و الزامات سازمان؛

ث- توصیه می‌شود به گونه‌ای پیاده‌سازی شوند تا امکان پایش، ارزشیابی و بهبود کارایی و اثربخشی کنترل‌های امنیت اطلاعات در جهت حمایت از اهداف سازمان امکان پذیر شود. توصیه می‌شود، انتخاب و پیاده‌سازی 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 مشخص شده 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 برآورده‌سازی نیازهای خاص سازمان طراحی شود. ضروری است که تشخیص داده شود، برخی از کنترل‌ها ممکن است برای هر سیستم یا محیط اطلاعاتی قابل به‌کارگیری نباشد و ممکن است برای همه سازمان‌ها قابلیت به‌کارگیری 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 می‌شود، 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 پیش‌بینی شده است، مطلع شوند.

باید توجه داشت که هیچ مجموعه‌ای از کنترل‌ها منجر به تحقق کامل امنیت اطلاعات نمی‌شود، بلکه توصیه می‌شود 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 اثربخشی ISMS

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 بازنگری ISMS، 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، واریسی، 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 مستمر است، به عبارت دیگر اقدامات به صورت 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 در رسیدن به اهداف کسب و کار 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 از طرف تمامی سطوح مدیریت به خصوص مدیریت ارشد؛

ت- درک الزامات حفاظت دارای 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 خط‌مشی‌ها و استانداردهای امنیت اطلاعات مندرج شده و تشویق آن‌ها به رعایت این الزامات؛

ج- فرآیند مدیریت مؤثر رخدادهای 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 دارای‌های 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 می‌شود، مزایایی که برای سازمان‌ها محقق خواهد شد، عبارت‌اند از:

الف- چارچوب ساخت یافته جهت پشتیبانی از فرآیند مشخص سازی، پیاده سازی، بهره برداری و نگهداری ISMS یکپارچه، مقرون به صرفه جامع، ارزش آفرین و همسو که نیازهای سازمان را در بهره برداری ها و جایگاه های مختلف برآورده می کند؛

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 کسب و کار در مورد مدیریت کلان نگر^۱ امنیت اطلاعات؛

پ- ترویج اقدامات امنیت اطلاعات مطلوب و پذیرفته شده جهانی، با روش غیردستوری و آزادی عمل دادن به سازمان ها در پذیرش و بهبود کنترل های مرتبط با شرایط خاص آن ها که منطبق شود و به منظور نگهداری از آن ها در برابر تغییرات داخلی و خارجی؛ و

ت- تدارک زبان مشترک و مفاهیم پایه ای برای امنیت اطلاعات و کمک به ایجاد اطمینان در شرکای کاری در مورد ISMS مورد توافق، به خصوص اگر خواهان دریافت گواهی رعایت استاندارد ISO/IEC27001 از نهاد معتبر صدور گواهی^۲ باشند؛

ث- افزایش اعتماد ذی نفعان به سازمان؛

ج- تحقق نیازها و انتظارات اجتماعی؛

چ- مدیریت اقتصادی کارآمدتر سرمایه گذاری های امنیت اطلاعات.

۴ استانداردهای خانواده ISMS

۱-۴ اطلاعات کلی

استانداردهای خانواده ISMS شامل استانداردهای مرتبط باهم است که در گذشته منتشر شده اند یا در دست تدوین هستند و تعدادی از مؤلفه های ساختاری مهم را در برمی گیرند. این مؤلفه ها متمرکز بر استانداردهایی اجباری است که به توصیف الزامات ISMS (استاندارد ISO/IEC 27001) و همچنین الزامات نهاد صدور گواهی (استاندارد ISO/IEC27006) که انطباق با استاندارد ISO/IEC 27001 را تایید می کنند، به کار گرفته می شوند. سایر استانداردها، راهنمایی برای جنبه های مختلف پیاده سازی ISMS، پرداختن به فرآیند عمومی، رهنمودهای مرتبط با کنترل و راهنمایی های بخش های خاص را فراهم می کند.

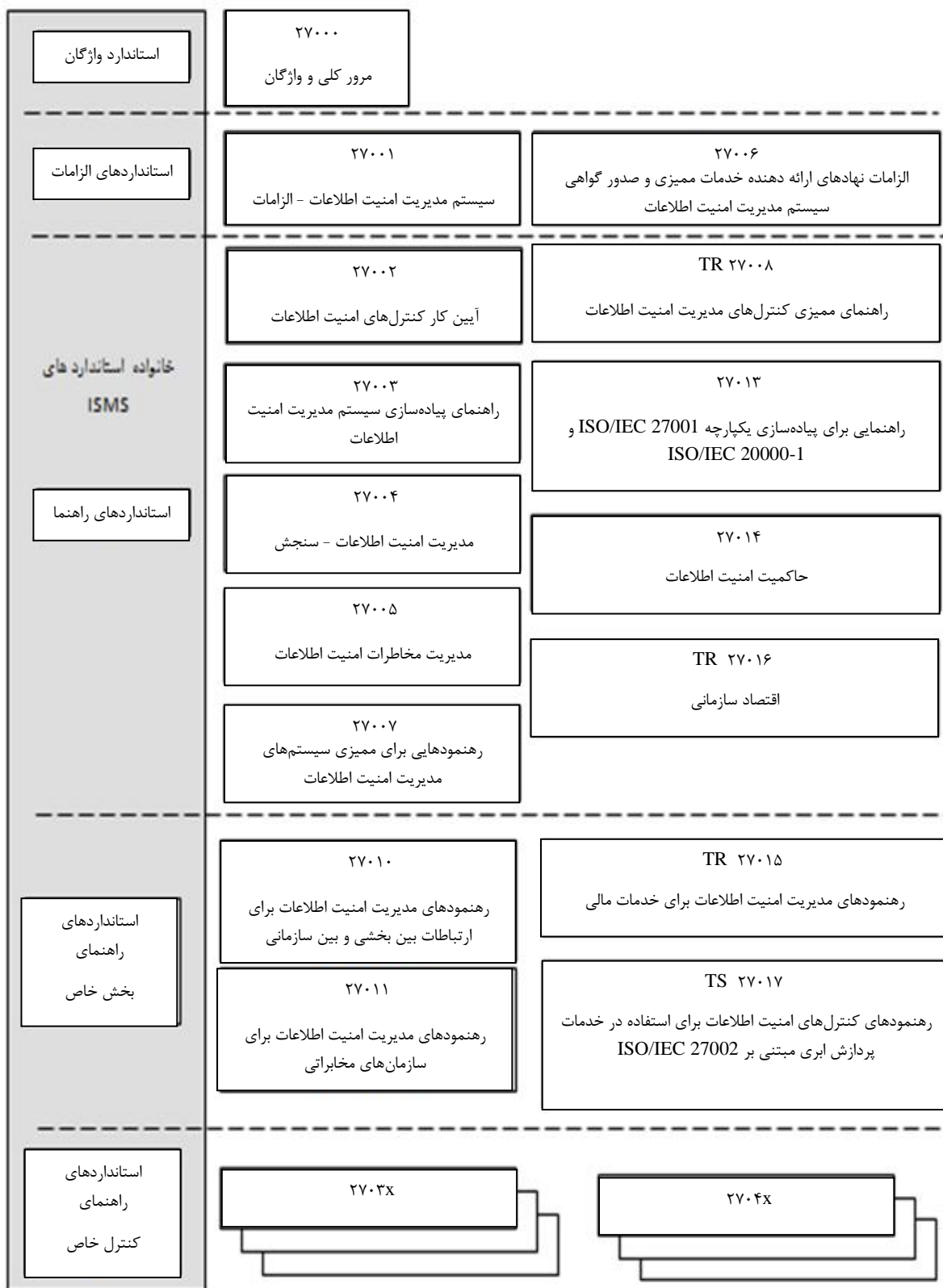
روابط استانداردهای خانواده ISMS در شکل ۱ نشان داده شده است.

الف- هر یک از استانداردهای خانواده ISMS برحسب نوع (یا نقش) آن در خانواده استانداردهای ISMS و شماره مراجع آن، در ادامه شرح داده شده است. بندهای کاربردی پذیر عبارتند از: استانداردهای توصیف کننده مرور کلی 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

۲-۴ استانداردهای توصیف‌کننده مرور کلی و واژگان

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

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

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

الف- مرور کلی بر استانداردهای خانواده ISMS؛

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

پ- اصطلاحات و تعاریف مورد استفاده 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.

۳-۴ استانداردهای مشخص‌کننده الزامات

۱-۳-۴ استاندارد ISO/IEC 27001^۱

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 در نظر گرفتن 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 صرف نظر 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

به منظور 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 گواهی شده باشند. اهداف کنترلی و کنترل‌های پیوست الف (استاندارد ISO/IEC 27001) باید به‌عنوان

قسمتی از این فرآیند ISMS انتخاب شوند تا الزامات شناسایی شده 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 استخراج شده 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.

۴-۳-۲ استاندارد ISO/IEC 27006^۱

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 گواهی ISMS 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 می‌شوند، 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 27002^۲

فناوری اطلاعات- فنون امنیتی- آیین کار کنترل‌های امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی، فهرستی از اهداف کنترلی پذیرفته‌شده معمول و کنترل‌های 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 به‌روشنی‌های پشتیبانی از کنترل‌های مشخص‌شده در بندهای الف-۵ تا الف-۱۸ ISO/IEC 27001 ارائه می‌دهد.

۲-۴-۴ استاندارد ISO/IEC 27003^۳

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.

۳-۴-۴ استاندارد ISO/IEC 27004^۱

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 مشخص شده 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 27005^۲

فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی، راهنمایی 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.

۵-۴-۴ 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 میزان سیستم مدیریت امنیت اطلاعات ارائه می‌کند.

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

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

۲- استاندارد ملی ایران با شماره ۲۷۰۰۵ ISIRI 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 مستقر شده 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 می‌دهد. 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 مشخص شده 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 پذیرفته شده است، ISO/IEC 27001 را پیاده‌سازی کنند، یا بالعکس؛

ب- هر دو استاندارد ISO/IEC 27001 و ISO/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 و ISO/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 تبدیل شده است. نه تنها 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.

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 شناسایی شده خود را تعیین کنند؛ ارزش مخاطرات بالقوه چنین دارایی‌ها را تعیین کنند؛ ارزشی که کنترل‌های حفاظت اطلاعات برای این دارایی‌های اطلاعاتی دارند را درک کنند و سطح بهینه منابعی را که جهت امن‌سازی 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 می‌کند. 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 بین‌المللی 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 بین‌المللی 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 27011^۱

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 سازگار یافته از دستورالعمل‌های ISO/IEC 27002 برای سازمان‌های مخابراتی که مختص همان صنعت تنظیم شده است را ارائه می‌کند و اضافه بر الزاماتی است که باید برای پاسخ به پیوست الف استاندارد ISO/IEC 27001 رعایت شوند.

۳-۵-۴ استاندارد ISO/IEC TR 27015^۱

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

دامنه کاربرد: این گزارش فنی علاوه بر راهنمایی‌های ارائه شده در خانواده استانداردهای ISMS، راهنمایی‌هایی جهت راه‌اندازی، پیاده‌سازی، نگهداری و بهبود امنیت در سازمان‌هایی که فراهم‌کننده خدمات مالی هستند، ارائه می‌کند.

هدف: این گزارش فنی مکمل اختصاصی استانداردهای بین‌المللی 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 تعریف‌شده در استاندارد بین‌المللی ISO/IEC 27002:2005 یا در استاندارد حاضر.

۴-۵-۴ استاندارد ISO 27799^۲

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

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

هدف: استاندارد ملی ایران شماره ۱۳۲۲۰، نسخه‌ای سازگار یافته از دستورالعمل‌های ISO/IEC 27002 برای سازمان‌های سلامت که مختص همان صنعت تنظیم شده 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 ISIRI ۱۳۲۲۰ در سال ۱۳۸۹ با منبع بین‌المللی ISO 27799:2008، منتشر شده است.

پیوست الف

(اطلاعاتی)

کاربرد افعال در بیان مقررات

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

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

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

نشانه	شرح
الزامات ^a	اصطلاحات «باید ^b » و «نباید ^c » دلالت بر الزاماتی دارد که به شدت دنبال می‌شوند تا مطابق با سند باشد و انحراف از آن مجاز نیست.
توصیه ^d	اصطلاحات «توصیه می‌شود ^e » و «توصیه نمی‌شود ^f » نشان‌دهنده این است که از میان چندین مورد ممکن، یک مورد به دلیل اینکه خصوصاً مناسب است، پیشنهاد می‌شود، بدون آن که به گزینه‌های دیگر اشاره یا آن‌ها را مستثنی کند یا این که عمل معینی برتری داده شود ولی نه اینکه حتماً 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 Permission ^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، استاندارد است که اصطلاح را در ابتدا تعریف کرده است. مالک اصطلاح همچنین مسئولیت نگهداری اصطلاح را بر عهده دارد، از جمله:

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

یادآوری ۱-ISO/IEC27001 خود، هرگز به عنوان مالک اصطلاح تلقی نمی شود.

یادآوری ۲-ISO/IEC 27001 و ISO/IEC 27006 به عنوان استانداردهای پایه (به عبارت دیگر، دربرگیرنده الزامات) همیشه به عنوان مالک غالب اصطلاح، مورد توجه قرار می گیرند.

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

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

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

Verification	۲-۸۸ درستی سنجی
	ISO/IEC 27005 ۲-۵ ب
Consequence	۲-۱۴ پیامد
Event	۲-۲۵ رویداد
External context	۲-۲۷ زمینه بیرونی
Internal context	۲-۴۲ زمینه 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 اطلاع رسانی 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 آسیب پذیری
	ISO/IEC 27006 ۲-۶ ب
Certificate	گواهی نامه
Certification body	نهاد صدور گواهی
Certification document	سند گواهی نامه

Mark	علامت
Organization	سازمان
	ISO/IEC 27007 ۷-۲-ب
Audit scope	۶-۲ محدوده کاربرد ممیزی
	ISO/IEC TR 27008 ۸-۲-ب
Review object	۶۶-۲ شیء موردبازنگری
Review objective	۶۷-۲ هدف بازنگری
Security implementation standard	۸۱-۲ استاندارد پیاده‌سازی امنیت
	ISO/IEC 27010 ۹-۲-ب
Information sharing community	۳۸-۲ جامعه اشتراک‌گذار اطلاعات
Trusted information communication entity	۸۵-۲ هستار مورد اعتماد ارتباط اطلاعات
	ISO/IEC 27011 ۱۰-۲-ب
Collocation	باهم گذاری
Communication centre	مرکز ارتباط
Essential communications	ارتباطات ضروری
Non-disclosure of communications	عدم افشاء ارتباطات
Personal information	اطلاعات شخصی
Priority 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
	ISO/IEC 27014 ۱۱-۲-ب
Executive management	۲۶-۲ مدیریت اجرایی
Governance of information security	۲۸-۲ حاکمیت امنیت اطلاعات
Governing body	۲۹-۲ نهاد حکومتی
Stakeholder	۸۲-۲ ذینفع
	ISO/IEC TR 27015 ۱۲-۲-ب
Financial services	خدمات مالی
	ISO/IEC 27016 ۱۳-۲-ب
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	ارزش افزوده اقتصادی
Economics	اقتصادی
Expected value	ارزش مورد انتظار
Extended value	ارزش تمدید شده
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

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

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

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

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

	ISO/IEC 27011 ۱۰-۲-ب
Telecommunications equipment room	اتاق تجهیزات مخابراتی
Essential communications	ارتباطات ضروری
Personal information	اطلاعات شخصی
Collocation	باهم گذاری
Terminal facilities	تسهیلات پایانه
Telecommunications facilities	تسهیلات مخابراتی
Perority call	تماس اولویت دار
Telecommunications services	خدمات مخابراتی
Telecommunications organizations	سازمان های 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	کسب و کار مخابراتی
Communication centre	مرکز ارتباط
Telecommunications service customer	مشتری خدمت مخابراتی
	ISO/IEC 27014 ۱۱-۲-ب
Governance of information security	۲۸-۲ حاکمیت امنیت اطلاعات
Stakeholder	۸۲-۲ ذینفع
Executive management	۲۶-۲ مدیریت اجرایی
Governing body	۲۹-۲ نهاد حکومتی
	ISO/IEC TR 27015 ۱۲-۲-ب
Financial services	خدمات مالی

	ISO/IEC 27016 ب-۲-۱۳
Value	ارزش
Societal value	ارزش اجتماعی
Economic value added	ارزش افزوده اقتصادی
Market value	ارزش بازار
Extended value	ارزش تمدید شده
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

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

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

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

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

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

پیوست ت
(اطلاعاتی)
واژگان فارسی به انگلیسی

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

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

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

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

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

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

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

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	اصالت سنجی
9	Authenticity	اصالت
10	Availability	دسترس پذیری
11	Base measure	سنجه مبنا
12	Certificate	گواهی نامه
13	Certification body	نهاد صدور گواهی
14	Certification document	سند گواهی نامه
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	ارزش افزوده 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)	برون سپاری کردن
87	Performance	عملکرد
88	Perority call	تماس اولویت دار
89	Personalinformation	اطلاعات شخصی
90	Policy	خط مشی
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	کسب و کار مخابراتی
119	Telecommunications equipment room	اتاق تجهیزات مخابراتی
120	Telecommunications facilities	تسهیلات مخابراتی
121	Telecommunications organizations	سازمان های 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	آسیب پذیری

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 information security management systems auditing
- [11] ISO/IEC TR 27008:2011, Information technology — Security techniques — Guidelines for auditor on information security controls
- [12] ISO/IEC 27010:2012, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications
- [13] ISO/IEC 27011:2008, Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- [14] ISO/IEC 27013:2012, Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- [15] ISO/IEC 27014:2013, Information technology — Security techniques — Governance of information security
- [16] ISO/IEC TR 27015:2012, Information technology — Security techniques — Information security management guidelines for financial services
- [17] ISO/IEC TR 27016-2, Information technology — Security techniques — Information security management — Organizational economics
- [18] ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002
- [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 management system requirements