ISIRI-ISO-IEC

27005

1st. edition

Identical with
ISO-IEC27005:2008

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ایران- ایزو - آی ای سی

۲۷۰۰۵

چاپ اول

فن‌آوری اطلاعات- فنون امنیتی- مدیریت ریسک امنیت اطلاعات

Information technology- Security techniques information security risk management

ICS:35.040

به نام خدا

آشنایی با سازمان استاندارد و تحقیقات صنعتی ایران

سازمان استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان 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.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان[۱]، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که سازمان استاندارد تشکیل می‌دهد به تصویب رسیده باشند.

سازمان استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[۲] کمیسیون بین‌المللی الکتروتکنیک (IEC)[۳] و سازمان بین‌المللی اندازه شناسی قانونی (OIML)[۴] است و به عنوان تنها رابط[۵] کمیسیون کدکس غذایی (CAC) [۶] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

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

۱- سازمان استاندارد و تحقیقات صنعتی ایران

2 - International organization for Standardization

3 - International Electro technical Commission

4 - International Organization for Legal Metrology (Organization International de Metrology Legal)

5 - Contact point

6 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فن‌آوری اطلاعات – فنون امنیتی – مدیریت ریسک امنیت اطلاعات»

رئیس:	**سمت و/ یا نمایندگی**
قرایی، محمد حسن (کارشناسی ارشد مخابرات - سیستم)	گروه مهندسین فن آوری نوین۵۲ (سهامی خاص)
دبیران:	
رضایی، امید (کارشناسی ارشد مخابرات - رمز)	گروه مهندسین فن آوری نوین۵۲ (سهامی خاص)
میرمطهری، سید نوید (کارشناسی ارشد مخابرات - سیستم)	گروه مهندسین فن آوری نوین۵۲ (سهامی خاص)
اعضاء: (اسامی به ترتیب حروف الفبا)	
احمدلو، یعقوب (کارشناسی ارشد مدیریت فنآوری اطلاعات)	کارشناس ارشد دفتر مرکزی حراست بانک کشاورزی
ارومیه چی ها، محمد علی (کارشناسی ارشد مخابرات - رمز)	کارشناسارشد شرکت صنایع الکترونیک زعیم
بلندقامت، حسین (کارشناس ارشد کامپیوتر - نرم افزار)	کارشناس ارشد سازمان بیمه ایران
تدین، محمدحسام (دکتری ریاضی کاربردی)	عضوهیأت علمی مرکزتحقیقات مخابرات ایران
حمزه لوئی منفرد، حسن (کارشناسی ریاضی کاربردی)	مدیرعامل شرکت مهندسی ایمن رایانه شرق (سهامی خاص)
قاسمی، حسین (کارشناسی ارشد مخابرات - رمز)	کمیته ملی برق و الکترونیک ایران (INEC)

قرائی، نرجس	کارشناس
(کارشناسی برق - قدرت)	گروه مهندسین فن آوری نوین۵۲(سهامی خاص)
کریمی، علیرضا	مدیرحوزه اجرائی
(کارشناسی ارشد مخابرات - رمز)	آزمایشگاه و مرکز تخصصی آپا - رمز
میری، سیدامیرمسعود	عضو هیأت علمی
(دکتری - مهندسی برق)	دانشگاه امام حسین (ع)
یزدیان، علی	رئیس دانشکده برق
(دکتری - مهندسی برق)	دانشگاه تربیت مدرس

فهرست مندرجات

پیش گفتار

استاندارد "فن‌آوری اطلاعات - فنون امنیتی - مدیریت ریسک امنیت اطلاعات" که پیش‌نویس آن در کمیسیون فنی مربوط، توسط مرکزتحقیقات مخابرات ایران، برمبنای روش تنفیذ مورد اشاره **در راهنمای ISO/IEC Guide21-1 (پذیرش منطقه‌ای یا ملی استانداردهای "بین‌المللی/ منطقه‌ای" و دیگر مدارک استاندارد)** به عنوان استاندارد ملی ایران، تهیه شده و در هشتاد و هفتمین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده ها مورخ ۱۳۸۸/۱۰/۲۳ مورد تصویب قرارگرفته‌است اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌گردد.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهدشد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرارخواهدگرفت. بنابراین همواره از آخرین تجدیدنظر آنها استفاده‌خواهدشد.

این استاندارد ملی براساس پذیرش استاندارد بین‌المللی به شرح زیر است:

ISO/IEC 27005:2008, "Information technology — Security techniques — Information security risk management"

مقدمه

این استاندارد رهنمودهایی[1] برای "مدیریت ریسک امنیت اطلاعات"[2] در یک سازمان - که به‌صورت خاص از الزامات یک "سامانه مدیریت امنیت اطلاعات"(ISMS)[3] بر اساس استاندارد ISO/IEC 27001 پشتیبانی می‌کند - فراهم می‌کند. در هر حال، این استاندارد هیچ روش‌شناسی[4] خاصی را برای مدیریت ریسک امنیت اطلاعات فراهم نمی‌کند. تعریف رویکرد[5] مدیریت ریسک هر سازمان - مثلا بر حسب دامنه کاربرد ISMS، زمینه مدیریت ریسک، یا بخش صنعتی - بر عهده خود سازمان است. تعدادی از روش‌شناسی‌های موجود، تحت چارچوب شرح داده شده در این استاندارد برای پیاده‌سازی الزامات یک ISMS قابل استفاده هستند.

این استاندارد مربوط به مدیران و کارکنانی است که نسبت به مدیریت ریسک امنیت اطلاعات در درون یک سازمان و - در جایی که مقتضی است - "طرف‌های بیرونی"[6] پشتیبانی‌کننده از اینگونه فعالیت‌ها، دغدغه دارند.

1 - Guidelines
2 - Information Security Risk Management
3 - Information Security Management System (ISMS)
4 - Methodology
5 - Approach
6 - External parties

فن‌آوری اطلاعات - فنون امنیتی - مدیریت ریسک امنیت اطلاعات

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین‌المللی ISO/IEC 27005:2008 تدوین شده است.

هدف از تدوین این استاندارد تعیین کردن رهنمودهایی برای مدیریت ریسک امنیت اطلاعات می باشد.

این استاندارد از مفاهیم[1] کلی توصیف شده در استاندارد ISO/IEC 27001 پشتیبانی کرده و برای کمک به پیاده‌سازی رضایت‌بخش امنیت اطلاعات بر اساس یک رویکرد مدیریت ریسک، طراحی شده است.

آگاهی نسبت به مفاهیم، مدل‌ها، فرآیندها و "اصطلاح شناسی‌های"[2] شرح‌داده‌شده در استانداردهای ISO/IEC 27001 و ISO/IEC 27002 برای درک کامل این استاندارد، مهم است.

این استاندارد، در هر سازمانی (مانند "بنگاه‌های اقتصادی"[3]، "آژانس‌های دولتی"[4] و "سازمان‌های غیرانتفاعی"[5]) که قصد مدیریت ریسک‌هایی که ممکن است امنیت اطلاعات سازمان را با مخاطره مواجه کنند را دارند، قابل اجرا است.

۲ مراجع الزامی

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

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

استفاده از مراجع الزامی زیر برای این استاندارد الزامی است:

2.1. ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements

2.2. ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management

کلیه بندهای استاندارد بین‌المللی ISO/IEC 27005:2008 در مورد این استاندارد، معتبر و الزامی است.

---

1 - Concepts
2 - Terminologies
3 - Commercial enterprises
4 - Government agencies
5 - Non-profit organizations