استاندارد ایران-
ایزو/آی ای سی ۲۱۸۲۷
چاپ اول

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان استاندارد و تحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

ISIRI-ISO/ IEC 21827
1st. Edition

Identical with ISO/IEC 21827: 2008

فناوری اطلاعات– فنون امنیتی–

مهندسی امنیت سامانه ها– مدل قابلیت رشد

(SSE-CCM®)

Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

ICS 35.040

به نام خدا

آشنایی با موسسه استاندارد وتحقیقات صنعتی ایران

موسسه استانداردوتحقیقات صنعتی ایران به موجب بندیک ماده ۳ قانون اصلاح قوانین ومقررات موسسه استانداردو تحقیقات صنعتی ایران،مصوب بهمن ماه ۱۳۷۱تنها مرجع رسمی کشور است که وظیفه تعین، تدوین ونشراستاندارد های ملی(رسمی) ایران را برعهده دارد .

تدوین استاندارد در حوزه های مختلف کمیسیون فنی مرکب ازکارشناسان موسسه* صاحب نظران مراکز وموسسات علمی، پژوهشی ، تولیدی واقتصادی آگاه ومرتبط انجام می شود وکوششی همگام بامصالح ملی و باتوجه به شرایط تولیدی، فناوری وتجاری است که از مشارکت اگاهانه ومنصفانه صاحبان حق ونفع ، شامل تولید کنندگان ، مصرف کنندگان ، صادرکنندگان ووارد‌کنندگان، مراکزعلمی وتخصصی، نهادها ، سازمان های دولتی وغیردولتی حاصل می شود.پیش نویس استاندارد های ملی برای نظر خواهی به مراجع ذی نفع و اعضاءکمسیون های فنی مربوطه ارسال می شود. وپس از دریافت نظرهاوپیشنهادها درکمیته ملی مرتبط با آن رشته طرح درصورت تصویب به عنوان استاندارد ملی(رسمی) ایران چاپ ومنتشر می شود .

پیش نویس استانداردهایی که موسسات وسازمانهای علاقه مند ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند در کمیته ملی طرح و بررسی ودر صورت تصویب، به عنوان استاندارد ملی (رسمی)چاپ ومنتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شود که براساس مفاد نوشته شده در استاندارد ملی ایران شماره ۵ تدوین ودرکمیته ملی استاندارد مربوطه که موسسه استاندارد تشکیل می دهد به تصویب رسیده باشد .

موسسه استاندارد وتحقیقات صنعتی ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] کمیسیون بین المللی الکتروتکنیک(IEC)[2] وسازمان بین المللی اندازه شناسی قانونی(OIML)[3] است وبه عنوان تنهارابط[4] کمیسیون کدکس غذایی(CAC)[5] درکشورفعالیت می کند . درتدوین استاندارد های ملی ایران ضمن توجه به شرایط کلی ونیاز مندی های خاص کشور ، از آخرین پیشرفت های علمی ، فنی وصنعتی جهان و استاندارد های بین المللی بهره گیری می شود.

موسسه استانداردوتحقیقات صنعتی ایران می تواندبارعایت موازین پیش بینی شده درقانون برای حمایت ازمصرف کنندگان،حفظ سلامت وایمنی فردی وعمومی،حصول اطمینان ازکیفیت محصولات وملاحظات زیست محیطی واقتصادی اجرای بعضی ازاستاندارد های ملی ایران را برای محصولات تولیدی داخل کشورو / یا اقلام وارداتی باتصویب شورای عالی استاندارد، اجباری نماید. موسسه می تواند به منظورحفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی ودرجه بندی آن را اجباری نماید.و همچنین برای اطمینان بخشیدن به استفاده کنندگان ازخدمات سازمان هاو موسسات فعال، در زمینه آموزش، مشاوره ، بازرسی، ممیزی وصدور گواهی سامانه های کیفیت ومدیریت زیست محیطی ، آزمایشگاه ها ومراکزکالیبراسیون(واسنجی) وسایل سنجش، موسسه استاندارد این گونه سازمان ها موسسات رابراساس ضوابط نظام تاییدصلاحیت ایران ارزیابی می کند ودرصورت احرازشرایط لازم،گواهی تایید صلاحیت با آنها اعطاء و برعملکرد آنها نظارت می کند. ترویج دستگاه بین المللی یکا های کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها وانجام تحقیقات کاربردی برای ارتقاع سطح استاندارد های ملی ایران از دیگر وظایف این موسسه است .

---

* موسسه استاندارد وتحقیقات صنعتی ایران

1- International Organization for standardization
2 -International Electrotechnical commission
3 - International Organization for Legal Metrology (Organization International de Metrology Legal)
4 – Contact point
5 – Codex Alimentarius commission

کمیسیون فنی تدوین استاندارد

" فناوری اطلاعات– فنون امنیتی– مهندسی امنیت سامانه ها– مدل قابلیت رشد (SSE-CCM®) "

رئیس:	**سمت و/یا نمایندگی**
محمودزاده، مرتضی (دکترای مدیریت سیستم)	شرکت سهامی عام کف
دبیران:	
اعتمادی، محمود (فوق لیسانس مدیریت صنعتی)	بنیاد آموزش های فنی و حرفه ای ایرانیان
نوتاش، فاطمه (لیسانس مهندسی کامپیوتر)	دانشگاه علمی کاربردی داروگر
اعضاء (به ترتیب حروف الفباء) :	
اعتمادی، فرناز (فوق لیسانس ریاضیات)	وزارت آموزش و پرورش
جعفری، اکرم (لیسانس مهندسی کامپیوتر)	وزارت تعاون
خاوری، سیامک (لیسانس مهندسی برق و الکترونیک)	وزارت ارتباطات و فناوری اطلاعات- سازمان تنظیم مقررات و ارتباط رادیوئی
شاه محمودی، بهزاد (لیسانس فیزیک)	موسسه استاندارد و تحقیقات صنعتی ایران
صدیق زاده، وریا (لیسانس مهندسی برق و الکترونیک)	شرکت توسعه شبکه خاورمیانه(MIDNET)

غیاثیان، علی (فوق لیسانس ارتباطات)	دانشگاه جامع علمی کاربردی
فرحزادی، سیدهادی (لیسانس مهندسی برق و الکترونیک)	شرکت مهاد صنعت
نوتاش، جواد (لیسانس مهندسی مکانیک)	شرکت جهاد توسعه منابع آب

پیش گفتار

استاندارد"فناوری اطلاعات– فنون امنیتی– مهندسی امنیت سامانه ها– مدل قابلیت رشد (SSE-CCM®)" که پیش نویس آن در کمیسیون فنی مربوط، توسط بنیاد آموزش های فنی و حرفه ای ایرانیان، بر مبنای روش تنفیذ مورد اشاره در راهنمای ISO/IEC Guide 21-1 (پذیرش منطقه ای یا ملی استانداردهای" بین المللی/ منطقه ای" و دیگر مدارک استاندارد) به عنوان استاندارد ملی ایران، تهیه و در یکصد و دهمین اجلاسیه کمیته ملی استاندارد رایانه و فراوری داده ها مورخ ۱۳۸۹/۹/۸ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین ومقررات سازمان استاندارد وتحقیقات صنعتی ایران مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می گردد.

برای حفظ همگامی وهماهنگی با تحولات و پیشرفت های ملی وجهانی در زمینه صنایع، علوم و خدمات، استاندارد های ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استاندارد ها ارائه شود، در هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین همواره از آخرین تجدید نظر آن ها استفاده خواهد شد.

این استاندارد ملی براساس پذیرش استاندارد بین المللی به شرح زیراست:

ISO/IEC 21827: 2008 , Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)

فناوری اطلاعات– فنون امنیتی– مهندسی امنیت سامانه ها– مدل قابلیت رشد (SSE-CCM®)

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین المللی ISO/IEC 21827:2008 تدوین شده است.

هدف از تدوین این استاندارد، تعیین مهندسی امنیت سامانه ها – مدل قابلیت رشد[1](SSE-CMM®)، می باشد. SSE-CMM® که یک مدل فرایند مرجع است برای الزامات پیاده سازی امنیت در یک سامانه و یا یک سری از سامانه های مرتبط که دامنه امنیت فن آوری اطلاعات[2](ITS) می باشد، تمرکز می کند.

SSE-CMM® در دامنه ITS ، بر روی فرایندهایی که سابقا برای دستیابی به امنیت فن آوری اطلاعات (ITS) مورد استفاده قرار می گرفتند و به ویژه روی رشد آن فرایندها تمرکز می کرد. در SSE-CMM® فرایندی خاص جهت استفاده به یک سازمان تحمیل نمی شود، بلکه فقط یک روش شناسی ویژه می باشد. هدف این است که سازمان استفاده کننده از SSE-CMM® ترجیحا از فرایندهای موجود خود که بر اساس دیگر دستورالعمل های مستند ITS می باشند، استفاده کند.

این هدف شامل موارد زیر می شود:

- فعالیت های مهندسی امنیت سامانه در جهت محصول ایمن یا سامانه ای مطمئن به چرخه کامل عمر تعریف مفاهیم ، تحلیل نیازمندی ها، طراحی، توسعه، یکپارچه سازی، نصب، به کاراندازی، نگهداری و به کاربردن مجدد می پردازد.
- الزامات برای توسعه دهندگان محصول، توسعه دهندگان و ادغام کنندگان سامانه های امنیتی، سازمان هایی که سرویس های امنیتی کامپیوتر و مهندسی امنیت کامپیوتر را تهیه می کنند.
- تمامی انواع سازمان های مهندسی امنیت، اعم از سازمان های تجاری، دولتی و فرهنگی در هر اندازه ای که باشند.

اینکه SE-CMM® یک مدل مشخص برای بهبود و ارزیابی قابلیت مهندسی امنیت است، بدان معنا نیست که مهندسی امنیت باید جدا از سایر نظام های مهندسی باشد. بر عکس، یکپارچه سازی رو به رشد SSE-CMM®، این موضوع را در نظر دارد که امنیت در سراسر نظام های مهندسی (مانند سامانه ها، نرم افزار و سخت افزار) نفوذ دارد و اجزای مدل را برای پرداختن به چنین مواردی

[1] - Systems Security Engineering- Capability Maturity Model(SSE-CMM®)
[2] -Information technology security.

مشخص می کند. ویژگی رایج "شیوه های هماهنگ سازی" [1] نیاز به یکپارچه سازی امنیت با همه نظام ها و گروه های درگیر در یک پروژه و یا درون یک سازمان را دارد. بطور مشابه، محیط فرایند"امنیت هماهنگ سازی" اهداف و مکانیزم هایی که در هماهنگ سازی فعالیت های مهندسی امنیت مورد استفاده قرار می گیرند را تعریف می نماید.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن ها 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، اصلاحیه ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه های بعدی آن ها مورد نظر است.

استفاده از مرجع زیر برای کاربرد این استاندارد الزامی است :

2-1 ISO/IEC 15504-2, Information technology — Process assessment — Part 2: Performing an assessment

کلیه بندهای استاندارد بین المللی ISO/IEC 21827:2008 در مورد این استاندارد معتبر و الزامی است.

[1] -Coordinate Practices