به نام خدا

پیاده سازی استاندارد جهانی امنیت اطلاعات

ISO/IEC 21827

فناوری اطلاعات،تکنیک های امنیتی،مهندسی امنیت سیستم ها،مدل بلوغ توانایی

مؤلف:

دکتر کیوان ربیع نژاد گنجی

مؤسسه فرهنگی هنری
دیباگران تهران

◂ عنوان کتاب: **پیاده سازی استاندارد جهانی امنیت اطلاعات**

ISO/IEC 21827 فناوری اطلاعات،تکنیک های امنیتی،مهندسی سیستم ها، مدل بلوغ توانایی

◂ مولف : دکتر کیوان ربیع نژادگنجی

◂ ناشر: موسسه فرهنگی هنری دیباگران تهران

◂ ویراستار: مهدیه مخبری

◂ صفحه آرایی: شبنم هاشم زاده

◂ طراح جلد: داریوش فرسایی

◂ نوبت چاپ: اول

◂ تاریخ نشر: ۱۴۰۱

◂ چاپ و صحافی: درج عقیق

◂ تیراژ: ۱۰۰ جلد

◂ قیمت: ۲۰۵۰۰۰۰ ریال

◂ شابک: ۰-۵۳۵-۲۱۸-۶۲۲-۹۷۸

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهستان، پلاک ۱۲۵۱-تلفن: ۶۶۴۱۰۰۴۶-۲۲۰۸۵۱۱۱

فروشگاههای اینترنتی دیباگران تهران :
WWW.MFTBOOK.IR
www.dibagarantehran.com

سرشناسه:ربیع نژاد گنجی،کیوان،۱۳۶۸-
عنوان و نام پدیدآور: پیاده سازی استاندارد جهانی امنیت اطلاعات ISO/IEC 21827 :فناوری اطلاعات،تکنیک های امنیتی،مهندسی امنیت سیستم ها ،مدل بلوغ توانایی/مولف: کیوان ربیع نژاد گنجی؛ ویراستار: مهدیه مخبری.
مشخصات نشر: تهران : دیباگران تهران :۱۴۰۰
مشخصات ظاهری:۳۹۶ ص:مصور،نمودار
شابک: ۰-۵۳۵-۲۱۸-۶۲۲-۹۷۸
وضعیت فهرست نویسی: فیپا کتابنامه.
عنوان دیگر: فناوری اطلاعات،تکنیک های امنیتی،مهندسی امنیت سیستم ها،مدل بلوغ توانایی.
موضوع: مهندسی سیستم ها Systems engineering
موضوع: سیستم های کنترل هوشمند
موضوع: Intelligence control systems
رده بندی کنگره:۱۶۸ TA
رده بندی دیویی:۶۲۰/۰۰۱۱۷۱
شماره کتابشناسی ملی:۸۷۷۸۲۷۹

نشانی تلگرام:@mftbook نشانی اینستاگرام دیبا dibagaran_publishing

فهرست مطالب

بخش اول

ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827)

بخش دوم

راهنما و خودارزیابی ISO/IEC 21827

مقدمه ناشر

خط مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی با کیفیت عالی است که بتواند خواسته های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم وسرعت توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه، نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که دردست‌دارید تألیف "**جناب آقای دکتر کیوان ربیع نژاد گنجی** " است که با تلاش همکاران ما درنشر دیباگران تهران منتشرگشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات وخواسته های خود،به ما کمک کنید تا بهتر و دقیق تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم.برای رساندن پیام هایتان به ما از رسانه های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
dibagaran@mftplus.com

مقدمه مولف

ایزو[1] مخفف نام سازمان بین‌المللی[2] می‌باشد. مؤسسه بین‌المللی استانداردسازی (ایزو) یک فدراسیون بین‌المللی متشکل از نهادهای ملی استانداردها است. تعداد این سازمان‌ها بالغ بر 165 نهاد است، که هر کدام مختص یک کشور می‌باشد و نماینده این سازمان در ایران به نام INSO[3] شناخته شده‌است. ایزو یک سازمان غیردولتی می‌باشد که در سال 1947 میلادی تأسیس شده‌است.

ایزو استانداردهایی را برای طیف وسیعی از محصولات، مواد و فرآیندها توسعه داده و چاپ می‌کند. کاتالوگ استانداردهای این سازمان تقریباً به 97 زمینه تقسیم می‌شود، که شامل فناوری مراقبت‌های بهداشتی، مهندسی راه‌آهن، جواهرات، پوشاک، متالورژی، سلاح، رنگ، مهندسی عمران، کشاورزی و هواپیما می‌شود. ایزو علاوه بر تولید استانداردها، گزارش‌های فنی، مشخصات فنی، مشخصات در دسترس عموم، اصلاحات فنی و راهنماها را نیز منتشر می‌کند.

ایزو با ارائه استانداردهای مشترک بین کشورهای مختلف نقش مهمی در تسهیل تجارت جهانی ایفاء می‌کند. این استانداردها برای اطمینان از اینکه محصولات و خدمات ایمن، قابل اعتماد و باکیفیت هستند، در نظر گرفته شده‌است. برای کاربر نهایی و مصرف‌کننده، این استانداردها تضمین می‌کند که محصولات گواهی‌شده با حداقل استانداردهای بین‌المللی مطابقت دارند. این سازمان با تعیین بیش از بیست‌هزار استاندارد، از محصولات تولیدی و فناوری گرفته تا استانداردهای ایمنی مواد غذایی، کشاورزی و مراقبت‌های بهداشتی اعتبار دارد.

ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827) که در این کتاب به شرح آن پرداخته‌ایم، یک استاندارد بین‌المللی بر اساس مدل «بلوغ توانایی مهندسی امنیت سیستم‌ها»[4] است، که توسط انجمن بین‌المللی مهندسی امنیت سیستم‌ها[5] توسعه و چاپ شده‌است. ایزو 21827 مهندسی امنیت سیستم‌ها، مدل بلوغ توانایی را مشخص می‌کند، که ویژگی‌های ضروری برای موفقیت فرآیند مهندسی امنیت یک سازمان را توصیف می‌نماید. این استاندارد برای همه سازمان‌های مهندسی امنیت؛ از جمله دولتی، تجاری و دانشگاهی قابل اجرا است. ایزو 21827 فرآیند یا توالی خاصی را تجویز نمی‌کند؛ اما شیوه‌هایی را که عموماً در صنعت مشاهده می‌شود، نشان می‌دهد.

---

[1] ISO
[2] International Standard Organization
[3] Iran National Standards Organization
[4] SSE-CMM
[5] ISSEA

این مدل یک معیار استاندارد برای شیوه‌های مهندسی امنیت است، که موارد زیر را پوشش می‌دهد:

- چرخه عمر پروژه؛ از جمله فعالیت‌های توسعه، بهره‌برداری، تعمیر و نگهداری و ازکارافتادن
- کل سازمان‌ها؛ از جمله فعالیت‌های مدیریتی، سازمانی و مهندسی
- تعامل همزمان با سایر رشته‌ها؛ مانند نرم‌افزار و سخت‌افزار سیستم، عوامل انسانی، مهندسی آزمون، مدیریت، بهره‌برداری و نگهداری سیستم
- تعامل با سایر سازمان‌ها؛ از جمله اکتساب، مدیریت سیستم، صدور گواهینامه، اعتبارسنجی و ارزیابی.

این کتاب در دو بخش سعی بر توضیح استاندارد ISO/IEC 21827 با پایبند بودن به بندهای اصلی این استاندارد جهانی و فراهم آوردن راهنمایی برای تعیین، ارزیابی و پیاده‌سازی درست این استاندارد در سازمان یا کسب‌وکار مورد نظر دارد.

در بخش اول کتاب شرح استاندارد ISO IEC 21827 را خواهیم داشت و در بخش دوم با سوال‌های خودارزیابی مبتنی بر استاندارد ISO IEC 21827 می‌توانیم برداشت صحیحی از اجرای درست کمی و یا کیفی کار داشته باشیم و پاسخ پرسش‌های زیر را به دست آوریم.

- دلایل تجاری قانع‌کننده برای شروع ISO IEC 21827 چیست؟
- آیا ISO IEC 21827 در حال حاضر طبق برنامه برنامه‌ریزی شده‌است؟
- آیا ساختار حاکمیت ISO IEC 21827 موجود است؟
- چگونه می‌دانید که پروژه ISO IEC 21827 موفق بوده‌است؟
- آیا به افرادی که بیش‌ترین تأثیر را در ایجاد خدمات/محصولات عالی ISO IEC 21827 دارند، به شدت پاداش می‌دهیم و تبلیغ می‌کنیم؟

پیش‌نویس ISO IEC 21827

ISO (سازمان بین‌المللی استاندارد) و IEC (کمیسیون بین‌المللی الکتروتکنیک) سیستم تخصصی استانداردسازی در سراسر جهان را تشکیل می‌دهند. نهادهای ملی که عضو ISO یا IEC هستند از طریق کمیته‌های فنی که توسط سازمان مربوطه برای رسیدگی به زمینه‌های خاص فعالیت فنی ایجاد می‌شود، در توسعه استانداردهای بین‌المللی شرکت می‌کنند. کمیته‌های فنی ISO و IEC در زمینه‌های مورد نظر مشترک با یکدیگر همکاری می‌کنند. سایر سازمان‌های بین‌المللی، دولتی و غیردولتی، در ارتباط با ISO و IEC نیز در این کار مشارکت دارند. در زمینه فناوری اطلاعات، ISO و IEC یک کمیته فنی مشترک به نام JTC IEC/ISO ایجاد کرده‌اند.

استانداردهای بین‌المللی مطابق با قوانین مندرج در بخش 2 دستورالعمل IEC/ISO تهیه می‌شوند.

وظیفه اصلی کمیته فنی مشترک تهیه استانداردهای بین‌المللی است. پیش‌نویس استانداردهای بین‌المللی تصویب‌شده توسط کمیته فنی مشترک برای رأی‌گیری در اختیار نهادهای ملی قرار داده می‌شود. چاپ و تأیید یک استاندارد بین‌المللی مستلزم تأیید حداقل 75 درصد از نهادهای ملی است، که رأی می‌دهند.

توجه داشته باشید، که برخی از عناصر این سند ممکن است موضوع حقوق ثبت اختراع باشد. ISO و IEC مسئولیتی در قبال شناسایی هیچ یک یا همه این حقوق ثبت‌شده نخواهند داشت.

ISO/IEC 21827 توسط کمیته فنی مشترک JTC IEC/ISO 1، فناوری اطلاعات، کمیته فرعی 27 SC و تکنیک‌های امنیت فناوری اطلاعات تهیه شده‌است. علاوه بر این، هم‌راستایی با مهندسی امنیت سیستم عمومی- مدل بلوغ توانایی نسخه 3، که توسط انجمن مهندسی امنیت سیستم‌های بین‌المللی به عنوان یک مستند با دسترسی عمومی منتشر شده‌است، حفظ می‌شود.

ویرایش دوم نسخه اول را لغو کرده و جایگزین (ISO/IEC 21827:2002) می‌شود، که از نظر فنی بازنگری شده‌است.

SSE-CMM؛ شامل گزیده‌هایی از «مدل بلوغ توانایی مهندسی سیستم (SE-CMM)، نسخه 1,1»، CMU/SEI—95-MM-003، حق چاپ 1955 توسط دانشگاه کارنگی ملون است.

SE-CM یک کار مشترک از شرکت‌های:

- Hughes Space and Communications،
- Hughes Telecommunications and Space،
- Lockheed Martin ،Engineering Institute Software،
- Software Productivity Consortium و
- Texas Instruments.

است. نه دانشگاه کارنگی ملون و نه مؤسسه مهندسی نرم‌افزار به طور مستقیم یا غیرمستقیم SSE-CMM یا ISO/IEC 21827 را تأیید نمی‌کنند.