



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**



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

## ◀ 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 نژاد گنجی

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ ویراستار: مهدیه مخبری

◀ صفحه آرای: 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: ۹۷۸-۶۲۲-۲۱۸-۵۳۵-۰

◀ نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱-تلفن: ۰۴۶-۶۶۴۱۰۰۴۶-۲۲۰۸۵۱۱۱

◀ فروشگاههای اینترنتی دیباگران تهران :

**WWW.MFTBOOK.IR**

**www.dibagaran-tehran.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: ۹۷۸-۶۲۲-۲۱۸-۵۳۵-۰  
وضعیت فهرست نویسی: فیا 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: ۰۱۱۷۱: ۶۲۰/۰۰  
شماره کتابشناسی ملی: ۸۷۷۸۲۷۹

نشانی اینستاگرام دیبا dibagaran\_publishing @mftbook: نشانی تلگرام:

هر کتاب دیباگران، یک فرصت جدید علمی و شغلی.

هر گوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

# فهرست مطالب

## بخش اول

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

24	..... مقدمه
24	..... 0,1 کلیات
25	..... ارائه‌دهندگان خدمات امنیتی
25	..... طراحان اقدام متقابل
25	..... طراحان محصول
26	..... بخش‌های خاص صنعتی
26	..... 0,2 چطور باید از SSE-CMM® استفاده کرد؟
27	..... 0,3 مزایای استفاده از SSE-CMM®
29	..... فناوری اطلاعات، تکنیک‌های امنیتی، مهندسی امنیت سیستم‌ها، مدل بلوغ توانایی (SSE-CMM®) ..
29	..... 1-هدف
30	..... 2-منابع معیاری
30	..... 3-اصطلاحات و تعاریف

30	3,1 پاسخگویی
30	3,2 اعتبار گذاری
31	3,3 ارزیابی
31	3,4 دارایی
31	3,5 تضمین
31	3,6 بحث تضمین
32	3,7 ادعای ضمانت
32	3,8 شواهد تضمین
32	3,9 اعتبار
32	3,10 سهولت دسترسی
33	3,11 خط مینا
33	3,12 صدور گواهی
33	3,13 قابلیت اعتماد
33	3,14 پایداری
34	3,15 صحت و درستی
34	3,16 مشتری
34	3,17 اثربخشی
34	3,18 گروه مهندسی
35	3,19 اسناد
35	3,20 یکپارچگی اجزاء

35	.....	3,21	سرویس و نگهداری
35	.....	3,22	شیوه کار
35	.....	3,23	مشخصات نفوذ
35	.....	3,24	رویه کار
36	.....	3,25	پردازش
36	.....	3,26	پایایی
36	.....	3,27	خطر باقی مانده
36	.....	3,28	خطر
37	.....	3,29	تحلیل ریسک
37	.....	3,30	مدیریت ریسک
37	.....	3,31	سیاست امنیت
37	.....	3,32	شرایط مرتبط با امنیت
38	.....	3,33	سیستم
38	.....	3,34	تهدید
38	.....	3,35	عامل تهدید
39	.....	3,36	تعیین اعتبار
39	.....	3,37	تأیید
39	.....	3,38	آسیب پذیری
39	.....	3,39	خروجی کار

40	4-پیش‌زمینه
40	4,1 علل توسعه
41	4,2 اهمیت مهندسی امنیت
41	4,3 وفاق جمعی
43	5-ساختار سند
43	6- ساختار مدل
43	6,1 مهندسی امنیت
46	6,2 بازبینی فرآیند مهندسی امنیت
51	6,3 شرح ساختار SSE-CMM®
64	6,4 خلاصه نمودار
66	7-شیوه‌های پایه امنیت
67	7,1 PA01 اجرای کنترل‌های امنیت
73	7,2 PA02- ارزیابی اثر مخرب
80	7,3 PA03- ارزیابی ریسک امنیت
85	7,4 PA04- ارزیابی تهدید
91	7,5 PA05- ارزیابی آسیب‌پذیری
97	7,6 PA06- ایجاد بحث تضمین
103	7,7 PA07- هماهنگی امنیت
107	7,8 PA08- نظارت بر وضع امنیت
115	7,9 PA09- ارائه خروجی امنیت
122	7,10 PA10- نیازهای خاص امنیتی

129.....	PA11 7,11- تأیید و معتبر شناختن امنیت
134.....	پیوست A
134.....	پیوست B
134.....	B.1 کلیات
135.....	B.2 ملاحظات امنیتی عمومی
135.....	B.2.1 ریسک پروژه در برابر ریسک امنیت
135.....	B.2.2 قابلیت اجرا در مرحله عملیاتی
135.....	B.2.3 مهندسی امنیت در برابر مهندسی سیستم‌ها
136.....	B.2.4 روابط مهندسی
136.....	B.3 PA12- تضمین کیفیت
136.....	B.3.1 حوزه فرآیند
138.....	B.3.2 BP.12.01- شناسایی نیازهای کیفی خروجی پروژه
139.....	B.3.3 BP.12.02- نظارت بر همسان بودن فرآیند تعریف شده
139.....	B.3.4 BP.12.03- اندازه‌گیری کیفیت خروجی پروژه
140.....	B.3.5 BP.12.04- اندازه‌گیری کیفیت فرآیند
141.....	B.3.6 BP.12.05- تحلیل اندازه‌گیری‌های کیفیت
142.....	B.3.7 BP.12.06- فراهم کردن مشارکت
143.....	B.3.8 BP.12.07- آغاز فعالیت‌های بهبود کیفیت
143.....	B.3.9 BP.12.08- شناسایی نیاز به اقدامات اصلاحی
144.....	B.4 PA13- مدیریت پیکربندی‌ها
144.....	B.4.1 حوزه فرآیند

- 146.....BP.13.01 :B.4.2 - برپایی شیوه مدیریت پیکربندی
- 147.....BP.13.02 :B.4.3 - شناسایی واحدهای پیکربندی
- 148.....BP.13.03 :B.4.4 - حفظ مبانی خروجی پروژه
- 149.....BP.13.04 :B.4.5 - کنترل تغییرات
- 149.....BP.13 :B.4.6 - انتقال وضعیت پیکربندی
- 150.....PA14 B.5 - مدیریت ریسک‌های پروژه
- 150.....B.5.1 حوزه فرآیند
- 152.....BP.14.01 :B.5.2 - طراحی رویکرد مدیریت ریسک
- 153.....BP.14.02 :B.5.3 - شناسایی ریسک‌ها
- 154.....BP.14.03 :B.5.4 - ارزیابی ریسک‌ها
- 155.....BP.14.04 :B.5.5 - مرور ارزیابی ریسک
- 155.....BP.14.05 :B.5.6 - اجرای کاهش شدت ریسک
- 156.....BP.14.06 :B.5.7 - پیگیری اقدام به کاهش شدت ریسک
- 157.....PA15 B.6 - نظارت و کنترل اقدام فنی
- 157.....B.6.1 حوزه فرآیند
- 159.....BP.15.01 :B.6.2 - هدایت اقدام فنی
- 159.....BP.15.02 :B.6.3 - پیگیری منابع پروژه
- 160.....BP.15.03 :B.6.4 - پیگیری پارامترهای فنی
- 160.....BP.15.04 :B.6.5 - بازبینی عملکرد پروژه
- 161.....BP.15.05 :B.6.6 - تحلیل مسائل پروژه
- 162.....BP.15.06 :B.6.7 - دست به اقدام اصلاحی زدن



- 163..... PA16 B.7 - طراحی اقدام فنی
- 163..... B.7.1 حوزه فرآیند
- 164..... BP.16.01:B.7.2 - شناسایی منابع حیاتی و مهم
- 165..... BP.16.02:B.7.3 - برآورد دامنه پروژه
- 166..... BP.16.03:B.7.4 - برآورد هزینه‌های پروژه
- 167..... BP.16.04:B.7.5 - تعیین فرآیند پروژه
- 167..... BP.16.05:B.7.6 - شناسایی فعالیت‌های فنی
- 168..... B.16.06:B.7.7 - تعریف واسط پروژه
- 169..... BP.16.07:B.7.8 - تهیه زمان‌بندی‌های پروژه
- 170..... BP.16.08:B.7.9 - تهیه پارامترهای فنی
- 171..... BP.16.09:B.7.10 - تهیه طرح مدیریت فنی
- 171..... BP.16.10:B.7.11 - بازبینی و تأیید طرح‌های پروژه
- 172..... PA17 B.8 - تعرف فرآیندهای مهندسی سیستم سازمان
- 172..... B.8.1 حوزه فرآیند
- 174..... BP.17.01:B.8.2 - تعیین اهداف فرآیند
- 175..... BP.17.02:B.8.3 - جمع‌آوری دارایی‌های فرآیند
- 176..... BP.17.03:B.8.4 - تهیه فرآیند مهندسی سیستم‌های سازمان
- 177..... BP.17.04:B.8.5 - تعریف دستورالعمل‌های متناسب‌سازی
- 178..... PA18 B.9 - بهبود فرآیندهای مهندسی سیستم‌های سازمان
- 178..... B.9.1 حوزه فرآیند
- 179..... BP.18.01:B.9.2 - ارزیابی فرآیند

- 180.....BP.18.02:B.9.3- طراحی اصلاحات فرآیند
- 181.....BP.18.03:B.9.4- تغییر فرآیند استاندارد
- 181.....BP.18.04:B.9.5- اطلاع‌رسانی از اصلاحات فرآیند
- 182.....PA19 B.10- مدیریت تکامل خط تولید
- 182.....B.10.1 حوزه فرآیند
- 183.....BP.19.01:B.10.2- تعریف تکامل محصول
- 184.....BP.19.02:B.10.3- شناسایی فناوری‌های تولید جدید
- 185.....BP9.03:B.10.4- سازگار کردن فرآیندهای توسعه
- 185.....BP.19.04:B.10.5- اطمینان از دسترسی داشتن به مؤلفه‌های مهم
- 186.....PA20 B.11- مدیریت محیط پشتیبانی مهندسی سیستم‌ها
- 186.....B.11.1 حوزه فرآیند
- 188.....BP.20.01:B.11.2- حفظ آگاهی فنی
- 188.....BP.20.02:B.11.3- تعیین نیازهای پشتیبانی
- 189.....BP.20.03:B.11.4- به دست آوردن محیط پشتیبانی مهندسی سیستم‌ها
- 190.....BP.20.04:B.11.5- سازمان دادن محیط پشتیبانی مهندسی سیستم‌ها
- 190.....BP.20.05:B.11.6- گنجاندن فناوری جدید
- 191.....BP20.06:B.11.7- حفظ محیط
- 192.....BP.20.07:B.11.8- نظارت بر محیط پشتیبانی مهندسی سیستم‌ها
- 193.....PA21 B.12- ارائه دانش و مهارت مستمر
- 193.....B.12.1 حوزه فرآیند
- 194.....BP.21.01:B.12.2- شناسایی نیازهای آموزشی

- 195.....انتخاب سبک کسب دانش یا مهارت‌ها -BP.21.02 :B.12.3
- 196.....اطمینان از در دسترس بودن مهارت‌ها و دانش -BP.21.03 :B.12.4
- 197.....تهیه مطالب آموزشی -BP.21.04 :B.12.5
- 198.....آموزش کارکنان -BP.21.05 :B.12.6
- 199.....ارزیابی اثربخشی آموزش -BP.21.06 :B.12.7
- 200.....نگهداری سوابق آموزش -BP.21.07 :B.12.8
- 201.....هماهنگی با فروشندگان -PA22 B.13
- 201.....حوزه فرآیند -B.13.1
- 202.....شناسایی مؤلفه‌ها یا خدمات سیستم‌ها -BP.22.01 :B.13.2
- 203.....انتخاب فروشنده یا کمپانی‌های فروش -BP.22.03 :B.13.4
- 204.....بیان انتظارات -BP.22.04 B.13.5
- 205.....حفظ ارتباطات -BP.22.05 B.13.6
- 206.....پیوست C
- 206.....کلیات C.1
- 206.....بهبود فرآیند C.2
- 208.....نتایج مورد انتظار C.3
- 208.....بهبود قابلیت پیش‌بینی C.3.1
- 208.....بهبود کنترل C.3.2
- 209.....بهبود اثربخشی فرآیند C.3.3
- 209.....سوء تفاهات مشترک C.4
- 209.....مدل‌های CMM® فرآیند مهندسی را تعریف می‌کنند. C.4.1

210.....	C.4.2 مدل‌های CMM® کتاب‌های راهنما یا راهنماهای آموزشی هستند.
210.....	C.4.3 مدل SSE-CMM® جایگزینی برای ارزیابی محصول است
210.....	C.4.4 اسناد خیلی زیادی لازم است.
211.....	C.5 فاهیم کلیدی
211.....	C.5.1 مقدمه
211.....	C.5.2 سازمان‌ها و پروژه‌ها
212.....	C.5.3 سیستم
213.....	C.5.4 خروجی پروژه
213.....	C.5.5 مشتری
214.....	C.5.6 فرآیند
214.....	C.5.7 حوزه فرآیند
214.....	C.5.8 عدم وابستگی نقش
215.....	C.5.9 قابلیت فرآیند
215.....	C.5.10 نهادینه‌سازی
215.....	C.5.11 مدیریت فرآیند
216.....	C.5.12 مدل بلوغ قابلیت
216.....	D پیوست
216.....	D.1 کلیات
218.....	D.2 قابلیت سطح 1- اجرای غیررسمی
218.....	D.2.1 خصوصیات مشترک سطح قابلیت
218.....	D.2.2 خصوصیت مشترک 1,1- شیوه‌های پایه اجرا می‌شوند.

- D.3 قابلیت سطح 2- برنامه‌ریزی و پیگیری شده ..... 219
- D.3.1 خصوصیات مشترک سطح قابلیت ..... 219
- D.3.2 خصوصیت مشترک 2,1- برنامه‌ریزی عملکرد ..... 220
- D.3.4 خصوصیت مشترک 2,3- بازبینی عملکرد ..... 225
- D.3.5 خصوصیت مشترک 2,4- پیگیری عملکرد ..... 227
- D.4 قابلیت سطح 3- کاملاً تعریف شده ..... 229
- D.4.1 خصوصیات مشترک میزان قابلیت ..... 229
- D.4.2 خصوصیت مشترک 3,1- تعریف یک فرآیند استاندارد ..... 229
- D.4.3 خصوصیت مشترک 3,2- اجرای فرآیند تعریف شده ..... 231
- D.4.4 خصوصیت مشترک 3,3- هماهنگ‌سازی شیوه‌ها ..... 233
- D.5 قابلیت سطح 4- کنترل کمی ..... 237
- D.5.1 خصوصیات مشترک سطح قابلیت ..... 237
- D.5.2 خصوصیت مشترک 4,1- تعیین اهداف کیفی قابل اندازه‌گیری ..... 238
- D.5.3 خصوصیت مشترک 4,2- مدیریت عینی عملکرد ..... 239
- D.6 قابلیت سطح 5- بهبود مستمر ..... 240
- D.6.1 خصوصیت مشترک قابلیت سطح ..... 240
- D.6.2 خصوصیت مشترک شماره 5,1- بهبود قابلیت سازمانی ..... 241
- D.6.3 خصوصیت مشترک 5,2- بهبود اثربخشی فرآیند ..... 242

246.....	راهنمای کامل خودارزیابی
246.....	نحوه استفاده از خودارزیابی
247.....	ISO IEC 21827
247.....	مثال کارت امتیازی
249.....	شروع خودارزیابی
249.....	معیار شماره 1: تشخیص
256.....	معیار شماره 2: تعریف
268.....	معیار شماره 3: اندازه‌گیری
281.....	معیار شماره 4: تجزیه و تحلیل
289.....	معیار شماره 5: بهبود
301.....	معیار شماره 6: کنترل
312.....	معیار شماره 7: پایداری
341.....	منشور پروژه
341.....	گزارش وضعیت پیمانکار
342.....	ماتریس پیگردپذیری شرایط لازم
342.....	طرح مدیریت زمانبندی
343.....	اعلام دامنه رسیدگی پروژه
344.....	گزارش عملیات تغییر
345.....	کاربرگ تخمین مدت زمان لازم

- 345..... نظارت و کنترل گروه فرآیند
- 346..... احتمال و ماتریس اثر مخرب
- 347..... توافقنامه عملیات تیم
- 348..... طرح مدیریت پروژه
- 348..... طرح مدیریت کیفیت
- 349..... سندسازی شرایط لازم
- 350..... نمودار شبکه‌ای
- 351..... ویژگی‌های فعالیت
- 351..... معیارهای استاندارد کیفی
- 352..... وضعیت ارزش کسب‌شده
- 353..... برآورد مدت زمان فعالیت
- 354..... طرح مدیریت منابع انسانی
- 355..... مدیریت پرتفولیوی پروژه
- 356..... طرح مدیریت دامنه رسیدگی
- 356..... حسابرسی کیفیت
- 357..... واژه‌نامه WBS
- 358..... طرح مدیریت تدارکات
- 359..... طرح مدیریت سهامدار
- 360..... ارزیابی عملکرد اعضای تیم
- 361..... راه‌اندازی گروه فرآیند
- 361..... بستن گروه فرآیند

362.....	گزارش عملکرد پروژه
363.....	فهرست مراحل مهم
364.....	پیمناى هزینه
365.....	پدرخواست تغییر
365.....	پ نیازمندی‌ها به منابع فعالیت
366.....	پثبت فهرست مسائل
367.....	برآورد هزینه‌های فعالیت
368.....	ثبت فهرست تصمیمات
368.....	ارزیابی احتمال و اثر
369.....	فهرست راهنمای تیم
370.....	ثبت ریسک
371.....	ساختار تفکیک منابع
371.....	ساختار تفکیک کار
372.....	نقش‌ها و مسئولیت‌ها
373.....	ماتریس واگذاری مسئولیت
374.....	شرح فرضیات و محدودیت‌ها
375.....	صفحه داده‌های ریسک
375.....	بازبینی ریسک
376.....	طرح مدیریت نیازمندی‌ها
377.....	کاربرگ برآورد هزینه
378.....	زمان‌بندی پروژه



379.....	طرح بهبود فرآیند.....
380.....	طرح مدیریت ریسک.....
380.....	گروه اجرایی فرآیند.....
381.....	تحلیل اختلاف.....
382.....	اتمام قرارداد.....
382.....	پذیرش رسمی.....
382.....	طرح مدیریت هزینه.....
383.....	ماتریس تحلیل سهامدار.....
384.....	فهرست فعالیت.....
384.....	طرح مدیریت تغییر.....
385.....	حسابرسی تدارکات.....
386.....	آموخته‌ها.....
386.....	ارزیابی عملکرد تیم.....
387.....	ثبت‌نام سهامدار.....
388.....	گروه برنامه‌ریزی فرآیند.....
388.....	گزارش وضعیت اعضای تیم.....
389.....	طرح مدیریت ارتباطات.....
390.....	خاتمه پروژه یا مرحله.....
390.....	معیارهای انتخاب منبع.....



**مراجع بر اساس دسته‌بندی موضوعی**

392..... Security Engineering References

393.....Security Engineering Process Area References

394..... Systems/Software Process References

394..... Capability Maturity Model References

396..... Further References

خط‌مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی با کیفیت عالی است که تواند  
خواسته‌های 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.

گسترده‌گی علوم و سرعت 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 زمینه‌های گوناگون و مورد نیاز جامعه تلاش نموده  
برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار  
دهد.

کتابی که در دست‌دارید تألیف "جناب آقای دکتر کیوان ربیع نژاد گنجی" است که با تلاش همکاران  
ما در نشر دیباگران تهران منتشر گشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

**با نظرات خود مشوق و راهنمای ما باشید**

با ارائه نظرات و پیشنهادات و خواسته‌های خود، به ما کمک کنید تا بهتر و دقیق‌تر در جهت رفع  
نیازهای علمی و آموزشی کشورمان قدم برداریم. برای رساندن پیام‌هایتان به ما از رسانه‌های دیباگران  
تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره‌های تماس که در صفحه شناسنامه  
کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران  
dibagaran@mftplus.com

## مقدمه مولف

ایزو<sup>1</sup> مخفف نام سازمان بین‌المللی<sup>2</sup> 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<sup>3</sup> شناخته شده است. ایزو یک سازمان غیردولتی می‌باشد که در سال 1947 میلادی تأسیس شده است.

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 شده است. 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»<sup>4</sup> است، که توسط انجمن بین‌المللی مهندسی امنیت سیستم‌ها<sup>5</sup> توسعه و چاپ شده است. 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.

<sup>1</sup> ISO

<sup>2</sup> International Standard Organization

<sup>3</sup> Iran National Standards Organization

<sup>4</sup> SSE-CMM

<sup>5</sup> 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 شده است؟
- آیا ساختار حاکمیت ISO IEC 21827 موجود است؟
- چگونه می‌دانید که پروژه ISO IEC 21827 موفق بوده است؟
- 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 گزینه‌هایی 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,
- 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.