



جمهوری اسلامی ایران  
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization



استاندارد ملی ایران-ایزو-آی ای سی

۲۷۰۳۴-۱

چاپ اول

خرداد ۱۳۹۲

**INSO-ISO-IEC**

**27034-1**

**1st. Edition  
Identical with  
ISO/IEC 27034:2011  
Jun.2013**

فناوری اطلاعات- فنون امنیتی - امنیت

برنامه کاربردی

قسمت ۱: مرور کلی و مفاهیم

**Information technology — Security  
techniques — Application security—  
Part 1: Overview and concepts**

**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)<sup>۱</sup>، کمیسیون بین المللی الکتروتکنیک (IEC)<sup>۲</sup> و سازمان بین المللی اندازه شناسی قانونی (OIML)<sup>۳</sup> است و به عنوان تنها رابط<sup>۴</sup> کمیسیون کدکس غذایی (CAC)<sup>۵</sup> 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 سایل سنچش، 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 سایل سنچش، تعیین عیار 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 – امنیت برنامه کاربردی - قسمت ۱: مرور کلی و مفاهیم »

#### رئیس:

فولادیان، مجید

(فوق لیسانس مهندسی برق مخابرات)

#### سمت و/یا نمایندگی

مشاور سازمان فناوری اطلاعات ایران

#### دبیر:

میراسکندری، سید محمدرضا

(لیسانس مهندسی کامپیوتر نرم افزار)

مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات

#### اعضا : (اسامی به ترتیب حروف الفبا)

بختیاری، شیرین

(لیسانس مهندسی برق )

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

جمیل پناه، ناصر

(فوق لیسانس مدیریت)

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

خواجه امیری، هیلدا

( فوق لیسانس زبان شناسی)

مدرس مجتمع فنی تهران

سلطانی حقیقت، الهه

(لیسانس مهندسی برق مخابرات)

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

سعیدی، عذرا

(دانشجو دکتری مهندسی برق مخابرات)

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

عسگرزاده، مجید

(فوق لیسانس مهندسی کامپیوتر)

مدیر پروژه موسسه تحقیقات ارتباطات و فناوری اطلاعات

طی نیا، رضا

(فوق لیسانس مدیریت فناوری اطلاعات)

مدیر عامل شرکت مهندسی کاربرد سیستم سدید

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

فرهاد شیخ احمد، لیلا  
(فوق لیسانس مهندسی کامپیوتر نرم افزار)

کارشناس مسؤول تدوین استاندارد و امنیت شبکه

فیاضی، مهدی  
(لیسانس مهندسی برق الکترونیک)

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

قسمتی، سیمین  
(فوق لیسانس فناوری اطلاعات)

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

معروف، سینا  
(لیسانس مهندسی کامپیوتر - سخت افزار)

رئیس اداره تدوین استانداردها و نظارت بر امنیت  
سرویس ها سازمان فناوری اطلاعات ایران

میرزایی رضایی، طیه  
(فوق لیسانس فیزیک)

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

موجبی، محمود  
(فوق لیسانس مهندسی برق مخابرات)

کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

ناپلیان، کامران  
(فوق لیسانس فناوری اطلاعات)

عضو هیأت علمی دانشگاه امام حسین (ع)

ناصری، علی  
(دکتری برق مخابرات)

مدیر پروژه موسسه تحقیقات ارتباطات و فناوری اطلاعات

وکیلی، اسد الله  
(فوق لیسانس مهندسی کامپیوتر)

## فهرست مندرجات

صفحه	عنوان
ز	پیش‌گفتار
ح	۰-مقدمه
ح	۰-۱ کلیات
ط	۰-۲ هدف
ی	۰-۳ مخاطبان هدف
ل	۰-۴ اصول
ن	۰-۵ ارتباط با سایر استانداردهای بین‌المللی
۱	۱-هدف و دامنه کاربرد
۱	۲-مراجع الزامی
۲	۳-اصطلاحات و تعاریف
۷	۴-اصطلاحات کوتاه‌نوشت
۷	۵-ساختار استاندارد ISO/IEC 27034
۹	۶-مقدمه ای بر امنیت برنامه کاربردی
۹	۶-۱ کلیات
۹	۶-۲ امنیت برنامه کاربردی در برابر امنیت نرم افزار
۹	۶-۳ محدوده امنیت برنامه
۱۲	۶-۴ نیازهای امنیت برنامه کاربردی
۱۴	۶-۵ مخاطره
۱۵	۶-۶ هزینه های امنیت
۱۵	۶-۷ محیط هدف
۱۶	۶-۸ کنترل ها و اهداف آنها
۱۶	۷-فرآیندهای کلی استاندارد ISO/IEC 27034
۱۶	۷-۱ اجزاء، فرآیندها و چارچوب ها
۱۷	۷-۲ فرآیند مدیریت ONF
۱۸	۷-۳ فرایند مدیریت امنیت برنامه کاربردی
۲۰	۸-مفاهیم

۲۰	۸-۱ چارچوب الزامی سازمان
۴۳	۸-۲ ارزیابی مخاطره امنیت برنامه کاربردی
۴۵	۸-۳ چارچوب الزامی برنامه کاربردی
۴۹	۸-۴ فراهم کردن مقدمات و اجرای برنامه کاربردی
۵۴	۸-۵ ممیزی امنیتی برنامه کاربردی
۵۷	پیوست الف (اطلاعاتی) نگاشت فرایند توسعه موجود در مطالعه موردی استاندارد ملی ISO/IEC 27034
۷۷	پیوست ب (اطلاعاتی) نگاشت برنامه کاربردهای کنترل‌های امنیتی با یک استاندارد موجود
	پیوست پ (اطلاعاتی) فرایند مدیریت مخاطره در استاندارد ملی ایران به شماره 27005 مطابق با فرایند کاربردی مدیریت امنیت
۹۰	
۹۳	کتابنامه

## پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی - امنیت برنامه کاربردی- قسمت ۱: مرور کلی و مفاهیم » که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در دویست و پنجاه و هفتمین اجلاس کمیته‌ی ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۱۳۹۱/۱۱/۰۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن‌ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهاد که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد. منبع و مأخذی که برای تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 27034-1:2011, Information technology — Security techniques Application security— Part 1: Overview and concepts

## ۱-۰ کلیات

سازمان‌ها باید برای باقی ماندن در کسب و کار، از زیرساخت‌های اطلاعاتی و فنی خود محافظت کنند. به طور سنتی، این مسئله در سطح فناوری اطلاعات به وسیله حفاظت از محیط و اجزای زیرساخت فنی فناوری مانند رایانه‌ها و شبکه‌ها که به طور کلی ناکافی هستند اداره شده‌است.

علاوه بر این، سازمان‌ها به طور فزاینده از خود در سطح حکومت با اجرا کردن سامانه‌های مدیریت امنیت اطلاعات (ISMS)<sup>۱</sup> رسمی، آزمایش و تایید شده حفاظت می‌کنند. طبق استاندارد ISO/IEC 27001، یک رویکرد نظام‌مند به سامانه موثر مدیریت امنیت اطلاعات کمک می‌کند.

با این حال سازمان‌ها با نیاز در حال رشد حفاظت از اطلاعات خویش در سطح برنامه کاربردی روبرو هستند. برنامه‌های کاربردی باید در مقابل آسیب‌پذیرهایی حفاظت شوند که ممکن است ذات برنامه کاربردی باشند (برای نمونه نقص نرم‌افزار)، در جریان چرخه حیات برنامه کاربردی (برای نمونه از طریق تغییرات برنامه کاربردی) ظاهر می‌شوند یا در اثر استفاده از برنامه کاربردی در زمینه‌ای که برای آن در نظر گرفته نشده‌است، به وجود می‌آیند.

یک رویکرد نظام‌مند برای افزایش امنیت برنامه کاربردی، شواهدی از حفاظت کافی اطلاعاتی که در حال استفاده یا ذخیره توسط برنامه‌های کاربردی سازمان هستند را فراهم می‌کند.

برنامه‌های کاربردی می‌توانند از طریق توسعه داخلی، برون سپاری یا خرید یک محصول تجاری به دست آیند. برنامه‌های کاربردی همچنین می‌توانند از طریق ترکیب این رویکردها به دست بیایند که ممکن است مفاهیم امنیت کاربردی جدیدی را معرفی نمایند که باید در نظر گرفته شده و مدیریت شوند.

نمونه‌هایی از این برنامه‌های کاربردی، سامانه‌های منابع انسانی، سامانه‌های مالی، سامانه‌های پردازش واژه، سامانه‌های مدیریت مشتریان، دیوار آتش، سامانه‌های ضد ویروس و سامانه‌های تشخیص نفوذ می‌باشد.

یک برنامه کاربردی امن در طول چرخه حیات خود، ویژگی‌های پیش نیاز از کیفیت نرم‌افزار مانند اجرای قابل پیش‌بینی و انطباق را نشان می‌دهد و همچنین الزامات امنیتی توسعه، مدیریت، زیرساخت فنی و دیدگاه ممیزی را برآورده می‌کند. فرایندها و تجارب امنیتی تقویت‌شده و افراد ماهری که آنها را انجام می‌دهند، باید برنامه‌های کاربردی قابل اطمینانی بسازند که در معرض مخاطره قرار گرفتن را از سطح قابل قبول و قابل تحمل مخاطره باقیمانده افزایش ندهند و از ISMS موثر استفاده کنند.

علاوه بر این یک برنامه کاربردی امن الزامات امنیتی ناشی از نوع داده‌ها، محیط هدف (حوزه کسب و کار، مقررات تنظیم‌شده و زمینه‌های فنی)، کنشگرها و مشخصات برنامه کاربردی را در نظر می‌گیرد. باید امکان نشان دادن شواهدی که مشخص می‌کنند مخاطره باقیمانده در سطح قابل قبول (یا قابل تحمل) کسب‌شده و نگهداری می‌شود وجود داشته باشد.

1- Information security management system



## ۲-۰ هدف

هدف از تدوین این مجموعه استاندارد کمک به سازمان‌ها در یکپارچه کردن کامل امنیت در سرتاسر چرخه حیات برنامه‌های کاربردی آنها توسط موارد زیر است:

- الف) ارائه مفاهیم، اصول، چارچوب‌ها، اجزا و فرایندها؛
- ب) فراهم کردن سازوکارهای فرایندگرا برای ایجاد الزامات امنیتی، ارزیابی مخاطرات امنیتی، اختصاص سطح اعتماد هدف گذاری شده و انتخاب کنترل‌های امنیتی و سنجش‌های تایید مربوطه؛
- پ) ارائه رهنمودهایی برای ایجاد معیارهای پذیرش به سازمان‌هایی که برنامه‌های کاربردی را برون سپاری می‌کنند یا به کار می‌گیرند و برای سازمان‌هایی که برنامه‌های کاربردی صرف سوم را خریداری می‌کنند.
- ت) فراهم کردن سازوکارهای فرایندگرا برای مشخص کردن، تولید و جمع‌آوری شواهد مورد نیاز برای نشان دادن اینکه برنامه‌های کاربردی آنها می‌توانند به‌طور ایمن در محیطی تعریف شده، استفاده شوند.
- ث) حمایت از مفاهیم کلی تعیین شده در استاندارد ISO/IEC 27001 و کمک به پیاده‌سازی رضایت‌بخش امنیت اطلاعات بر پایه رویکرد مدیریت مخاطره؛ و
- ج) فراهم کردن چارچوبی که به پیاده‌سازی کنترل‌های امنیتی تعیین شده در ISO/IEC 27002 و دیگر استانداردها کمک کند.

این استاندارد ملی در موارد زیر کاربرد دارد:

الف) در مورد نرم‌افزارهای زمینه‌ای برنامه کاربردی و فاکتورهای شرکت‌کننده‌ای که امنیت آن را تحت تأثیر قرار می‌دهند مانند داده‌ها، فناوری، فرایندهای چرخه حیات توسعه برنامه کاربردی، فرایندهای پشتیبان و کنشگرها به کار گرفته می‌شود.

ب) در مورد تمام سازمان‌ها از هر نوع و در هر اندازه (برای نمونه شرکت‌های تجاری، آژانس‌های دولتی، سازمان‌های غیرانتفاعی) که در معرض مخاطرات مربوط به برنامه‌های کاربردی هستند.

این استاندارد ملی در موارد زیر کاربرد ندارد:

- الف) ارائه رهنمودهای امنیت فیزیکی و شبکه؛
- ب) ارائه کنترل‌ها یا سنجش‌ها؛
- پ) ارائه مشخصات کدگذاری امن برای هرگونه زبان برنامه نویسی.

این استاندارد ملی :

الف) استاندارد توسعه نرم‌افزار کاربردی نیست؛

ب) استاندارد مدیریت پروژه برنامه کاربردی نیست؛

پ) استاندارد چرخه حیات توسعه نرم‌افزار نیست.

الزامات و فرایندهای مشخص شده در این استاندارد ملی برای پیاده‌سازی به شکل مجزا در نظر گرفته نشده‌اند بلکه برای پیاده‌سازی به شکل یکپارچه با فرایندهای موجود سازمان در نظر گرفته شده‌اند. به این منظور سازمان باید فرایندهای موجود و چارچوب‌های پیشنهاد شده توسط این استاندارد ملی را ترسیم کند تا تأثیر پیاده‌سازی این استاندارد ملی کاهش یابد.

پیوست الف نمونه‌ای را فراهم می‌کند که توضیح می‌دهد چگونه یک فرایند توسعه نرم‌افزار موجود می‌تواند در برخی اجزا و فرایندهای این استاندارد ملی ترسیم شود. به‌طور کلی هر سازمانی که از هرگونه چرخه حیات توسعه استفاده می‌کند، باید ترسیمی مانند ترسیم توصیف‌شده در پیوست الف را انجام دهد و اجزا و فرایندهای جامانده مورد نیاز را برای تطبیق با این استاندارد ملی اضافه کنند.

### ۳-۰ مخاطبان هدف

#### ۳-۰-۱ کلیات

مخاطبان مشروحه زیر در حین اجرای جایگاه‌های سازمانی تعیین‌شده خود از این استاندارد بهره می‌برند:

الف) مدیران

ب) تیم‌های تامین و عملیات

پ) کارکنان تیم کارفرما

ت) تأمین‌کنندگان

ث) ممیزان

#### ۳-۰-۲ مدیران

مدیران افراد درگیر در مدیریت برنامه کاربردی در طی چرخه حیات کامل آن هستند. مراحل قابل اجرای چرخه حیات برنامه کاربردی مراحل تأمین و تولید را شامل می‌شوند. نمونه‌هایی از مدیران عبارتند از:

الف) مدیران امنیت اطلاعات

ب) مدیران پروژه

پ) سرپرستان

ت) کارفرمایان نرم‌افزار

ث) مدیران توسعه نرم‌افزار

ج) مالکان برنامه کاربردی

چ) مدیران صف که بر کارکنان نظارت دارند.

به‌طور معمول لازم است مدیران:

الف) هزینه پیاده‌سازی و حفظ امنیت برنامه کاربردی را در برابر مخاطرات و بهایی که برای سازمان مطرح می‌کنند، متعادل کنند؛

ب) گزارش ممیزهایی که پیشنهاد قبول یا رد برنامه کاربردی را براساس اینکه آیا برنامه کاربردی سطح اطمینان هدف‌گذاری‌شده را کسب کرده و حفظ می‌کند بازبینی کنند؛

پ) از تطبیق با استانداردها، قوانین و مقررات طبق حوزه مقررات تنظیم‌شده برنامه کاربردی اطمینان حاصل کنند. (به زیربند ۸-۱-۲-۲ مراجعه شود).

ت) پیاده‌سازی برنامه کاربردی امن را سرپرستی کنند؛

ث) سطح اعتماد هدف‌گذاری‌شده را طبق حوزه خاص سازمان تصویب کنند؛

ج) مشخص کنند کدام یک از کنترل‌ها و سنجش‌های تأیید باید پیاده‌سازی و آزمایش شوند؛

- (چ) هزینه‌های درستی‌سنجی امنیت برنامه کاربردی را به حداقل برسانند؛
- (ح) سیاست‌ها و رویه‌های امنیتی یک برنامه کاربردی را ثبت کنند؛
- (خ) برای تمام کنشگرها آگاهی، آموزش و دید آگاهانه امنیتی فراهم کنند؛
- (د) اختیارات امنیت اطلاعات مناسب مورد نیاز سیاست‌ها و رویه‌های امنیت اطلاعات قابل به‌کارگیری را جای‌گذاری کنند؛ و
- (ذ) در تمام برنامه‌های امنیتی مربوط به سامانه در درون شبکه سازمان حضور داشته باشند.

### ۳-۳-۰ تیم‌های تأمین و عملیات

اعضای تیم‌های تأمین و عملیات (که در مجموع به‌عنوان گروه پروژه شناخته می‌شوند) افرادی درگیر در طراحی، توسعه و حفظ برنامه کاربردی در طول چرخه کامل حیات آن هستند. این افراد عبارتند از:

(الف) مهندسین معمار،

(ب) تحلیل‌گران،

(پ) برنامه‌نویسان،

(ت) آزمایش‌کنندگان،

(ث) سرپرستان سامانه،

(ج) سرپرستان پایگاه داده،

(چ) سرپرستان شبکه و

(ح) کارکنان فنی.

به‌طور معمول لازم است اعضا:

(الف) درک کنند کدام کنترل‌ها باید در هر مرحله از چرخه حیات برنامه کاربردی به‌کار گرفته شوند و چرا؛

(ب) درک کنند کدام کنترل‌ها باید در خور برنامه کاربردی پیاده‌سازی شوند؛

(پ) تاثیر معرفی کنترل‌ها را در فعالیت‌های توسعه، آزمایش و ثبت در چرخه حیات برنامه کاربردی به حداقل برسانند؛

(ت) اطمینان حاصل کنند که کنترل‌های معرفی‌شده الزامات سنجش‌های مربوطه را برآورده می‌کنند؛

(ث) به‌منظور مؤثر کردن توسعه، آزمایش و ثبت به ابزارها و بهترین تجارب دسترسی پیدا کنند؛

(ج) بازبینی گروهی را آسان کنند؛

(چ) در برنامه‌ریزی و تهیه راهبرد شرکت کنند؛

(ح) برای کسب کالاها و خدمات مورد نیاز (برای نمونه درخواست، ارزیابی و اعطای قراردادها) روابط کسب و کار ایجاد کنند؛ و

(خ) پس از پایان کار ترتیب امحای ارقام باقیمانده را بدهند. (برای نمونه مدیریت/امحا دارایی)

### ۴-۳-۰ کارفرمایان

این شامل تمام افراد درگیر در تهیه یک محصول یا خدمت می‌شود.

به‌طور کلی لازم است کارفرمایان:

- الف) درخواست‌های امحا که شامل الزامات کنترل‌های امنیتی می‌شود را آماده کنند؛
- ب) تأمین‌کنندگان مطابق با این الزامات را انتخاب کنند؛
- پ) شواهد کنترل‌های امنیتی به‌کار گرفته شده توسط خدمات برون‌سپاری را تأیید کنند؛ و
- ت) محصولات را با تأیید شواهد پیاده‌سازی صحیح کنترل‌های امنیت برنامه کاربردی ارزیابی کنند.

#### ۵-۳-۰ تأمین‌کنندگان

این شامل تمام افراد درگیر در تأمین یک محصول یا خدمت می‌شود.  
به‌طور کلی لازم است تأمین‌کنندگان:

- الف) از میان درخواست‌های پیشنهادی با الزامات امنیتی برنامه کاربردی موافقت کنند؛
- ب) کنترل‌های امنیتی مناسب را برای پیشنهادها با توجه به تأثیر آنها بر هزینه‌ها انتخاب کنند؛
- پ) شواهدی فراهم کنند مبنی بر اینکه کنترل‌های امنیتی مورد نیاز به درستی در محصولات یا خدمات پیشنهادی پیاده‌سازی شده‌اند؛

#### ۶-۳-۰ ممیزها

ممیزها افرادی هستند که لازم است:

- الف) محدوده و رویه‌های درگیر در سنجش تأیید کنترل‌های مرتبط را درک کنند؛
- ب) اطمینان حاصل کنند که نتایج ممیزی قابل تکرار هستند؛
- پ) فهرستی از سنجش‌های تأییدی تأسیس کنند که شواهدی فراهم کند مبنی بر این‌که برنامه کاربردی به سطح اعتماد هدف‌گذاری‌شده درخواست‌شده توسط مدیریت رسیده است؛ و
- ت) فرایندهای ممیزی استاندارد را بر پایه استفاده از شواهد قابل تأیید به‌کارگیرند.

#### ۷-۳-۰ کاربران

کاربران افرادی هستند که لازم است:

- الف) اعتماد داشته باشند که استفاده و اجرای برنامه کاربردی امن فرض شده است؛
- ب) اعتماد داشته باشند که یک برنامه کاربردی نتایج معتبری را به شکل مداوم و به موقع تولید می‌کند؛
- پ) اعتماد داشته باشند که کنترل‌ها و سنجش‌های تأییدی مرتبط به شکل صحیح طبق انتظار قرار گرفته و کار می‌کنند.

#### ۴-۰ اصول

##### ۱-۴-۰ امنیت یک الزام است

الزامات امنیتی برای هر مرحله از چرخه حیات یک برنامه کاربردی باید تعریف و تحلیل شوند، به درستی مورد خطاب قرار گیرند و به شکل پیوسته مدیریت شوند.  
با الزامات امنیتی برنامه کاربردی ( به زیربند ۶-۴ مراجعه شود). باید به همان شیوه برخورد با الزامات کارکرد، کیفیت و قابلیت استفاده (برای نمونه‌ای از مدل کیفیت به استاندارد ISO/IEC 9126 مراجعه شود).

برخورد کرد. علاوه بر این، الزامات مربوط به امنیت برای مطابقت با محدودیت‌های به‌وجود آمده در مخاطرات باقیمانده باید برقرار شوند.

مطابق استاندارد ISO/IEC/IEEE 29148 (در حال تدوین)، الزامات باید ضروری، صریح، غیرمبهم، مداوم، کامل، دقیق، امکان‌پذیر، قابل ردیابی و قابل تأیید باشند. همین ویژگی‌ها باید در مورد الزامات امنیتی به‌کار گرفته شوند. اغلب اوقات در اسناد پروژه‌های برنامه کاربردی با الزامات امنیتی مبهم مانند «توسعه‌دهنده باید تمام مخاطرات امنیتی مهم را کشف کند» مواجه می‌شویم.

#### ۴-۰-۲ امنیت برنامه کاربردی وابسته به زمینه است

امنیت برنامه کاربردی تحت تأثیر محیط هدف تعریف‌شده است. نوع و محدوده الزامات امنیتی برنامه کاربردی توسط مخاطراتی که برنامه کاربردی در معرض آنها قرار می‌گیرد مشخص می‌شود که خود این مخاطرات وابسته به سه زمینه هستند:

(الف) زمینه کسب و کار: مخاطرات خاص برخاسته از زمینه کسب و کار سازمان (شرکت مخابرات، شرکت حمل و نقل، دولت و غیره)؛

(ب) زمینه مقررات تنظیم‌شده: مخاطرات خاص برخاسته از مکان جغرافیایی که سازمان در آن مشغول کسب و کار است. (حقوق و سند مالکیت فکری، محدودیت‌های حفاظت رمزنگاری، حق کپی، قوانین و مقررات، قانون حریم خصوصی و غیره)؛

(پ) زمینه فنی: مخاطرات خاص فناوری‌های استفاده‌شده توسط سازمان در جریان کسب و کار مهندسی معکوس، امنیت ابزارهای ساخت، حفاظت از کد منبع، استفاده از کد از پیش تعریف‌شده طرف سوم، آزمایش امنیت، آزمایش نفوذ، بررسی حدود، بررسی کد، محیط فناوری اطلاعات و ارتباطات (ICT) که برنامه در آن اجرا می‌شود، فایل‌های تنظیمی داده‌های تعریف‌نشده، مزایای سامانه عامل برای نصب یا اجرای برنامه، نگهداری و انتشار امن و غیره.

حوزه فنی مشخصات فنی برنامه کاربردی را دربر می‌گیرد (کارکرد امنیتی، اجزای امن، پرداخت آنلاین، برقراری ارتباط امن، رمزنگاری، مدیریت مجوزها و غیره).

یک سازمان می‌تواند تأیید کند که یک برنامه کاربردی امن است اما این تأیید تنها برای این سازمان و در حوزه کسب و کار، مقررات تنظیم‌شده و فنی خاص آن معتبر است. چنانچه برای مثال زیرساخت فنی برنامه کاربردی تغییر کند یا برنامه کاربردی با همین مقصود در کشور دیگری استفاده شود، ممکن است این حوزه‌های جدید بر الزامات امنیتی و سطح اعتماد هدف‌گذاری‌شده تأثیر بگذارند. ممکن است کنترل‌های امنیت برنامه کاربردی موجود دیگر به درستی الزامات امنیتی جدید را مورد خطاب قرار ندهند و ممکن است برنامه کاربردی دیگر امن نباشد.

#### ۴-۰-۳ سرمایه‌گذاری مناسب برای امنیت برنامه کاربردی

هزینه‌های به‌کارگیری کنترل‌های امنیت برنامه کاربردی و انجام سنجش‌های ممیزی باید با سطح اعتماد هدف‌گذاری‌شده (به زیربند ۸-۱-۲-۶-۴ مراجعه شود) مورد نیاز توسط مالک برنامه کاربردی یا مدیریت متناسب باشد.

این هزینه‌ها می‌تواند به‌عنوان یک سرمایه‌گذاری در نظر گرفته شوند زیرا هزینه‌ها، مسئولیت‌پذیری‌های مالک برنامه‌های کاربردی و عواقب قانونی نقض‌های امنیتی را کاهش می‌دهند.

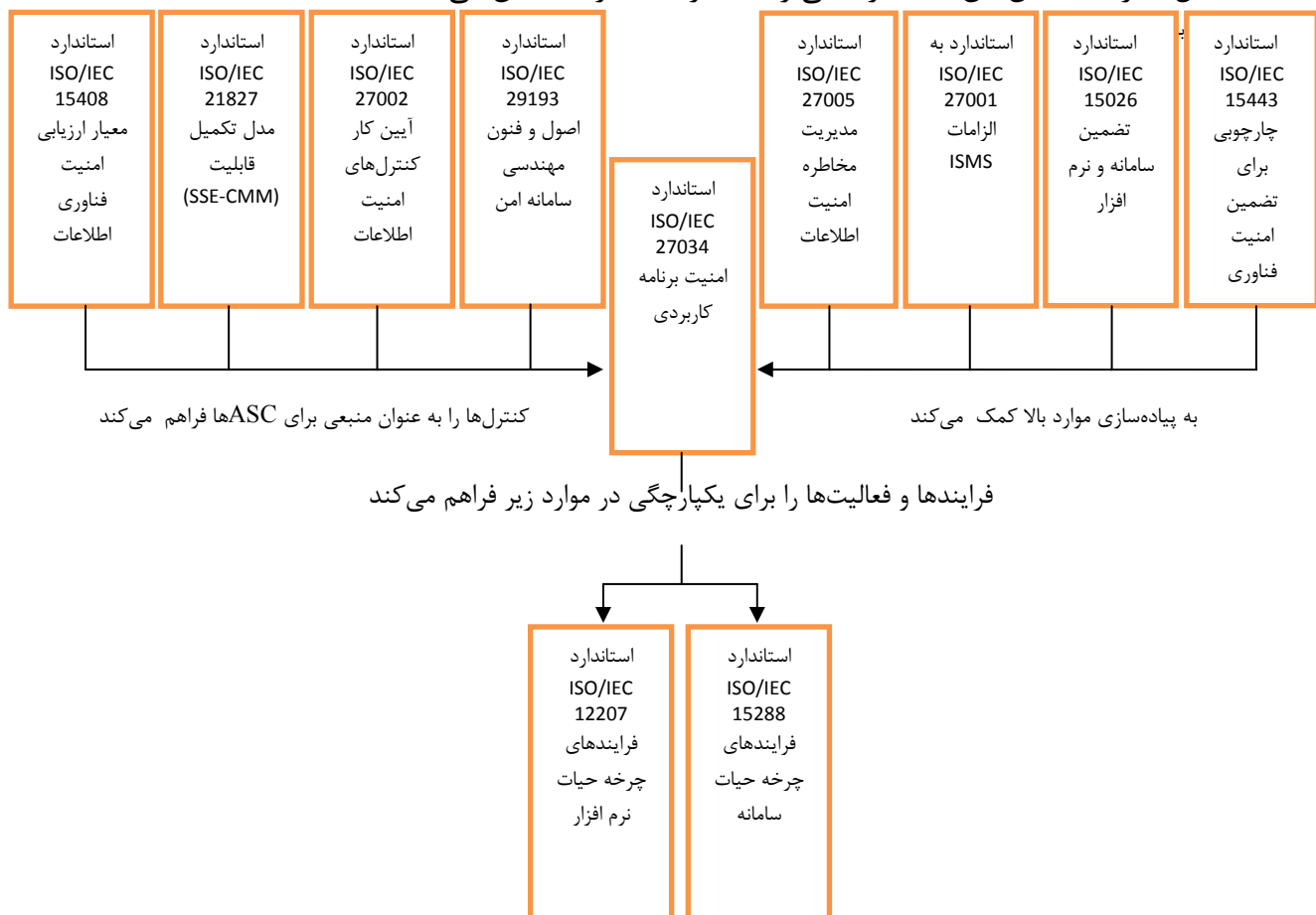
#### ۴-۴-۰ امنیت برنامه کاربردی باید اثبات شود

فرایند ممیزی برنامه کاربردی در این استاندارد ملی (به زیربند ۸-۵ مراجعه شود). از شواهد قابل تأیید فراهم‌شده توسط کنترل‌های امنیتی برنامه کاربردی استفاده می‌کند. (به زیربند ۸-۱-۲-۶-۵ مراجعه شود). یک برنامه کاربردی را نمی‌توان امن بیان کرد مگر اینکه ممیز موافقت کند که شواهد اثباتی حاصل سنجش‌های تأیید مرتبط کنترل‌های امنیت برنامه کاربردی نشان می‌دهند برنامه کاربردی به سطح اعتماد هدف‌گذاری‌شده مدیریت رسیده است.

#### ۵-۰ ارتباط با سایر استانداردهای بین‌المللی

##### ۵-۱ کلیات

شکل ۱ ارتباط میان این استاندارد ملی را با دیگر استانداردها نشان می‌دهد.



شکل ۱- ارتباط با سایر استانداردهای بین‌المللی

#### ۵-۲ استاندارد ISO/IEC 27001 سامانه‌های مدیریت امنیت اطلاعات- الزامات

استاندارد ISO/IEC 27004 با محدوده‌ای در حد امنیت برنامه کاربردی، به پیاده‌سازی پیشنهادات استاندارد ISO/IEC 27001 کمک می‌کند. به‌طور خاص رویکردهای زیر مورد استفاده قرار می‌گیرند:

الف) رویکردی نظام‌مند در مدیریت امنیت؛

ب) برنامه‌ریزی، انجام، بررسی و عمل به رویکرد فرایند؛ و

پ) پیاده‌سازی امنیت اطلاعات بر پایه مدیریت مخاطره

۵-۰-۳ استاندارد ISO/IEC 27002 ، فناوری اطلاعات - فنون امنیتی - آیین کار مدیریت امنیت اطلاعات

استاندارد ISO/IEC 27002 تجربه‌هایی را فراهم می‌کند که یک سازمان می‌تواند آنها را به‌عنوان کنترل‌های امنیت برنامه کاربردی پیشنهادشده توسط این استاندارد ملی پیاده‌سازی کند. کنترل‌های بندهای زیرین از استاندارد ISO/IEC 27002 مورد توجه بیشتری هستند:

الف) بند ۱۰: مدیریت ارتباطات و عملیات؛

ب) بند ۱۱: کنترل دسترسی؛ و مهم‌تر از همه

پ) بند ۱۲: تهیه، توسعه و حفظ سامانه‌های اطلاعاتی.

۵-۰-۴ استاندارد ISO/IEC 27005 - مدیریت مخاطرات امنیت اطلاعات

این استاندارد ملی با محدوده‌ای در حد امنیت برنامه کاربردی، به پیاده‌سازی فرایند مدیریت مخاطره پیشنهادشده توسط استاندارد ISO/IEC 27005 کمک می‌کند. برای بحث مفصل‌تر به پیوست پ (اطلاعاتی) مراجعه شود.

۵-۰-۵ استاندارد ISO/IEC 21827، مهندسی امنیت سامانه‌ها - مدل تکمیل قابلیت (SSE-CMM)

استاندارد ISO/IEC 21827 تجارب پایه مهندسی امنیتی را که یک سازمان می‌تواند به‌عنوان کنترل‌های امنیت اطلاعات برنامه کاربردی پیشنهادشده توسط این استاندارد ملی پیاده‌سازی کند، فراهم می‌کند. علاوه بر این، فرایندهای این استاندارد ملی در به‌دست آوردن بسیاری از قابلیت‌هایی که سطوح قابلیت استاندارد ISO/IEC 21827 را تعریف می‌کنند، کمک می‌کند.

۵-۰-۶ استاندارد ISO/IEC 15408-3 ، معیار ارزیابی امنیت فناوری اطلاعات - قسمت ۳: اجزای تضمین امنیت

استاندارد ISO/IEC 15408 الزامات و عناصر کنشگری را که سازمان می‌تواند به‌عنوان کنترل‌های امنیت برنامه کاربردی پیشنهادشده توسط این استاندارد پیاده‌سازی کند، فراهم می‌کند.

۵-۰-۷ استاندارد ISO/IEC 15443-1 ، چارچوبی برای تضمین امنیت فناوری اطلاعات - قسمت ۱: مرور کلی و چارچوب، و استاندارد ISO/IEC TR 15443 ، چارچوبی برای تضمین امنیت فناوری اطلاعات - قسمت ۳: شیوه‌های تحلیل تضمین

این استاندارد ملی به پیش‌برد و بازتاب اصول تضمین امنیت استاندارد ISO/IEC TR 15443-1 و مشارکت در پرونده‌های تضمینی ISO/IEC TR 15443-3 کمک می‌کند.

۵-۰-۸ استاندارد ISO/IEC 15026-2، مهندسی سامانه‌ها و نرم‌افزار - تضمین سامانه‌ها و نرم‌افزار - قسمت ۲: حالت تضمین

استفاده از فرایندها و کنترل‌های امنیت برنامه کاربردی این استاندارد ملی در پروژه‌های برنامه کاربردی به‌طور مستقیم پرونده‌های تضمینی راجع به امنیت برنامه کاربردی را تأمین می‌کند. به‌طور خاص:

الف) ادعاها و توجیهات آنها توسط فرایند تحلیل مخاطره امنیت برنامه کاربردی فراهم می‌شود،

ب) شواهد توسط سنجش‌های تأیید موجود کنترل‌های امنیت برنامه کاربردی تأمین می‌شوند، و

ج) تطابق با این استاندارد ملی می‌تواند در بسیاری از پرونده‌های تضمینی این چینی به‌عنوان استدلال استفاده شوند.

همچنین به زیربند ۸-۱-۲-۶-۵-۱ مراجعه شود.

**۹-۵-۰ استاندارد ISO/IEC 15288، مهندسی سامانه‌ها و نرم‌افزار - فرایندهای چرخه حیات سامانه و استاندارد ملی ISO/IEC 12207، مهندسی سامانه‌ها و نرم‌افزار - فرایندهای چرخه حیات نرم‌افزار**

این استاندارد ملی فرایندهای افزوده را برای سازمان و همچنین کنترل‌های امنیت برنامه کاربردی فراهم می‌کند که سازمان می‌تواند به‌عنوان فعالیت‌های افزوده در فرایندهای چرخه حیات مهندسی سامانه‌ها و نرم‌افزار موجود همان‌گونه که توسط استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207 فراهم شده است، وارد کند.

**۱۰-۵-۰ استاندارد ISO/IEC TR 29193 - (در حال توسعه)، اصول و فنون مهندسی سامانه امن**

استاندارد ISO/IEC TR 29193 برای مهندسی سامانه امن سامانه‌های ICT یا محصولاتی که سازمان می‌تواند همان‌گونه که توسط این استاندارد ملی پیشنهاد شده آنها را به‌عنوان کنترل امنیت برنامه کاربردی پیاده‌سازی کند، راهنمایی فراهم می‌کند.



## فناوری اطلاعات- فنون امنیتی- امنیت برنامه کاربردی

### قسمت ۱: مرور کلی و مفاهیم

#### ۱ هدف و دامنه کاربرد

هدف از تدوین استاندارد ملی، تعیین راهنمایی برای کمک به سازمان‌ها در یکپارچه سازی امنیت در فرایندهای مورد استفاده‌ی مدیریت برنامه‌های کاربردی آنها است.

این استاندارد مروری کلی بر امنیت برنامه کاربردی را ارائه می دهد و به تعاریف، مفاهیم، اصول و فرایندهای مورد بحث در امنیت برنامه می پردازد.

این استاندارد ملی برای برنامه‌های کاربردی توسعه داده شده داخلی، برنامه‌های کاربردی تهیه شده توسط طرف‌های سوم و نیز آنجا که توسعه یا عملیات برنامه، برون سپاری شده باشد، قابل استفاده 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 می شود.

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

استفاده از مراجع زیر برای این استاندارد الزامی است:

۱-۲ استاندارد ملی ایران به شماره ۲۷۰۰۰ : ۱۳۹۱ فناوری اطلاعات -فنون امنیتی -سامانه های مدیریت امنیت اطلاعات مرور کلی و واژگان

۲-۲ استاندارد ملی ایران به شماره ۲۷۰۰۱ : ۱۳۸۷ ، فناوری اطلاعات- فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات- الزامات

۳-۲ استاندارد ملی ایران به شماره ۲۷۰۰۲ : ۱۳۸۷ ، فناوری اطلاعات - فنون امنیتی -آیین کارمدیریت امنیت اطلاعات

۴-۲ استاندارد ملی ایران به شماره ۲۷۰۰۵ : ۱۳۹۱، فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات

### ۳ اصطلاحات و تعاریف

در این استاندارد ، علاوه بر اصطلاحات و تعاریف ارائه شده در استانداردهای ملی ایران به شماره‌های ، ISO/IEC 27001، ISO/IEC 27002 ، ISO/IEC 27005 اصطلاحات و تعاریف زیر نیز به کار می‌روند.

#### ۱-۳

#### کنشگر

شخص یا فرایندی است که فعالیتی را طی چرخه حیات یک برنامه کاربردی انجام می‌دهد یا عمل متقابلی را با هر فرایند فراهم‌شده توسط و یا متأثر از برنامه کاربردی آغاز می‌کند.

#### ۲-۳

#### سطح اعتماد واقعی

نتیجه حاصل از یک فرایند ممیزی است که دلایل اثبات کننده‌ای ارائه می‌کند که همه کنترل‌های امنیتی برنامه کاربردی، مورد نیاز برای سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی، به‌طور صحیح پیاده‌سازی و بازبینی شده و نتایج مورد نظر را ایجاد کرده‌اند.

#### ۳-۳

#### برنامه کاربردی

راه کار فناوری اطلاعات است که شامل نرم‌افزار برنامه کاربردی، داده و روش اجرایی برنامه کاربردی می‌شود و به‌منظور کمک به کاربران یک سازمان جهت انجام وظایف خاص یا سامان‌دهی انواع خاص مسائل فناوری اطلاعات با خودکارسازی یک فرایند یا کارکرد کسب و کار طراحی شده است.

یادآوری: فرایندهای کسب و کار مردم و فناوری‌ها را شامل می‌شود.

#### ۴-۳

#### مدل مرجع چرخه حیات امنیت برنامه کاربردی

مدل چرخه حیات مورد استفاده به‌عنوان مرجع برای معرفی فعالیت‌های امنیتی در فرایندها شامل مدیریت برنامه کاربردی، تولید و استفاده از برنامه کاربردی، مدیریت زیرساخت و ممیزی برنامه کاربردی است.

### ۵-۳

#### چارچوب الزامی برنامه کاربردی (ANF)<sup>۱</sup>

مجموعه عناصر الزامی مربوط به یک پروژه برنامه کاربردی خاص که از چارچوب الزامی سازمان انتخاب شده است.

### ۶-۳

#### مالک برنامه کاربردی

جایگاه سازمانی که مسئول مدیریت، به کارگیری و حفاظت برنامه کاربردی و اطلاعات آن است.

یادآوری ۱- مالک برنامه کاربردی تمامی تصمیمات مربوط به امنیت برنامه کاربردی را اتخاذ می کند.

یادآوری ۲- اصطلاح «مالک» در سراسر این این استاندارد به عنوان واژه مترادف برای «مالک برنامه کاربردی» به کار رفته است.

### ۷-۳

#### پروژه برنامه کاربردی

تلاشی است با معیارها و ضوابط معین آغاز و پایان که باید یک برنامه کاربردی مطابق با منابع و نیازهای خاص ایجاد کند.

منبع: [استاندارد ISO/IEC 12207، تعریف ۴-۲۹، اصلاح شده-تخصصی شده برای محدوده برنامه کاربردی]

یادآوری - برای اهداف این استاندارد، معیارهای آغاز و پایان به گونه ای هستند که کل چرخه حیات برنامه کاربردی را شامل می شوند.

### ۸-۳

#### کنترل امنیت برنامه کاربردی (ASC)<sup>۲</sup>

ساختمان داده ای شامل شماره دهی و توصیف دقیق یک فعالیت امنیتی و درستی سنجی مربوط به آن فعالیت امنیتی است که باید در نقطه خاصی از چرخه حیات یک برنامه کاربردی انجام شود.

---

1- Application Normative Framework  
2 - Application Security Control

۹-۳

### فرایند مدیریت امنیت برنامه کاربردی (ASMP)<sup>۱</sup>

کل فرایند مدیریتی برای فعالیت‌ها، کنشگرها، محصولات و ممیزی امنیتی هر برنامه کاربردی که مورد استفاده یک سازمان قرار می‌گیرد.

۱۰-۳

### نرم‌افزار برنامه کاربردی

نرم‌افزاری که به‌منظور کمک به کاربران در انجام وظایف خاص یا سامان‌دهی انواع خاصی از مسائل طراحی شده و متمایز از برنامه‌ای است که خود کامپیوتر را کنترل می‌کند.

[منبع: استاندارد ISO/IEC/IEEE 24765: 2010، تعریف ۱-۳.۱۳۰]

۱۱-۳

### ممیزی

فرایندی نظام‌مند و مستند برای حصول شواهد و ارزیابی عینی آن به‌منظور تعیین گستره‌ی برآورده‌شدن معیارهای سنجش.

[منبع: استاندارد ISO/IEC 9000: 2005، تعریف ۳-۹-۱، اصلاح شده - تعمیم یافته]

۱۲-۳

### محیط

زمینه کسب و کار، مقررات تنظیم‌شده و فنی که در آن یک برنامه کاربردی مورد استفاده قرار گرفته است. این محیط شامل همه فرایندها، محصولات، اطلاعات و کنشگرهای مورد بحث در برنامه کاربردی می‌شود.

۱۳-۳

### چرخه حیات

سیر تکامل تدریجی یک سامانه، محصول، خدمت، پروژه یا سایر موجودیت‌های انسان‌ساخت از آغاز شکل‌گیری تا زمان کنار گذاشته‌شدن آن است.

[منبع: استاندارد ISO/IEC 12207: 2008، تعریف ۴-۱۶]

۱۴-۳

### مدل چرخه حیات

چارچوب فرایندها و فعالیت‌های مرتبط با چرخه حیات که ممکن است به صورت چند مرحله‌ای سازمان‌دهی شده باشد. همچنین به عنوان مرجعی مشترک برای ارتباطات و ادراکات عمل می‌کند.

[منبع: استاندارد ISO/IEC 12207: 2008، تعریف ۱۷-۴]

۱۵-۳

### نگهداری

هر تغییری که در یک برنامه کاربردی، پس از تحویل و ارائه آن انجام شود. مثال‌ها: تصحیح خطا، کارکرد افزوده، بهبود عملکرد، ایجاد اطمینان از کارکرد برنامه کاربردی.

۱۶-۳

### چارچوب الزامی سازمان<sup>۱</sup> (ONF)

ساختار داخلی در سطح سازمان که شامل مجموعه‌ای از فرایندها و عناصر الزامی امنیت برنامه کاربردی می‌شود.

۱۷-۳

### کمیت چارچوب الزامی سازمان

جایگاه سازمانی مسؤول نگهداری و تصویب اجزای مرتبط با امنیت برنامه کاربردی در درون چارچوب الزامی سازمان.

۱۸-۳

### محیط بهره‌برداری

محیط بیرونی که وجود دارد یا انتظار می‌رود در طول اجرای یک برنامه کاربردی به وجود بیاید.

[منبع: استاندارد ISO/IEC 2382-7: 2000، تعریف ۷-۱۱-۷]

۱۹-۳

### محصول

### نتیجه‌ی یک فرایند

[منبع: استاندارد ISO/IEC 9000: 2005، تعریف ۳-۴-۲]

---

<sup>۱</sup> Organization Normative Framework

۲۰-۳

### برنامه کاربردی امن

برنامه کاربردی که سطح اعتماد واقعی آن برابر با سطح اعتماد هدف گذاری شده سازمانی است که برنامه کاربردی را استفاده می کند.

۲۱-۳

### سطح اعتماد هدف گذاری شده

نام یا برچسب مجموعه ای از کنترل های امنیت برنامه کاربردی که توسط مالک برنامه کاربردی به منظور کاهش مخاطره ای مربوط به یک برنامه کاربردی خاص تا سطح قابل قبول (یا قابل تحمل)، ضروری فرض شده اند، که این سطح اعتماد از یک تحلیل مخاطره امنیت برنامه کاربردی پیروی می کند.

۲۲-۳

### کاربر

شخصی که از چیزی استفاده می کند یا آن را اجرا می کند.

[ منبع: لغتنامه انگلیسی اکسفورد ]

یادآوری - برای اهداف این استاندارد، اصطلاح «کاربر» فقط شامل کاربر پایانی نمی شود بلکه شامل جایگاه های کاربردی و نگهداری از قبیل سرپرست سامانه و مجری پایگاه داده نیز می شود.

۲۳-۳

### اعتبار سنجی

تایید این که الزامات یک کاربرد برنامه ی خاص مورد نظر برآورده شده اند. این تایید از طریق ارائه شواهد عینی انجام می گیرد.

یادآوری ۱- اصطلاح «درستی سنجی شده» برای تعیین وضعیت متناظر به کار می رود.

یادآوری ۲- شرایط به کارگیری درستی سنجی می تواند واقعی یا شبیه سازی شده باشد.

[ منبع: استاندارد ISO/IEC 9000: 2005، تعریف ۳-۸-۵ ]

یادآوری ۳- در اصطلاح عامیانه، «درستی سنجی» به معنای این است که «آیا برنامه ساخته شده همان برنامه کاربردی مورد نظر است؟»

## درستی سنجی

تایید این که نیازهای مشخص برآورده شده‌اند. این تایید از طریق ارائه شواهد عینی انجام می‌گیرد.

یادآوری ۱- اصطلاح «درستی‌سنجی‌شده» برای تعیین وضعیت متناظر استفاده می‌شود.

یادآوری ۲- تایید می‌تواند شامل فعالیت‌هایی نظیر اجرای محاسبات متناوب، مقایسه مشخصات یک طرح جدید با مشخصات ثابت‌شده طرحی مشابه، پذیرش مسئولیت آزمون‌ها، نحوه اجرا و نیز بررسی اسناد پیش از نتیجه شود.

[منبع: استاندارد ISO/IEC 9000: 2005، تعریف ۳-۸-۴]

یادآوری ۳- در اصطلاح عامیانه، «درستی‌سنجی» به این معنا است که «آیا برنامه کاربردی به درستی در حال ساخت است؟»

## ۴ اصطلاحات و کوتاه‌نوشت‌ها

ANF	Application Normative Framework	چارچوب اصلی برنامه کاربردی
ASC	Application Security Control	کنترل امنیت برنامه کاربردی
ASMP	Application security Management Process	فرایند مدیریت امنیت برنامه کاربردی
COTS	Commercial Off The Shelf	نرم‌افزارهای تجاری و عمومی
ICT	Information and Communication Technology	فناوری اطلاعات و ارتباطات
ISMS	Information Security Management System	سامانه مدیریت امنیت اطلاعات
ONF	Organization Normative Framework	چارچوب الزامی سازمان
XML	eXtended Markup Language	سامانه نشانه‌گذاری گسترده

## ۵ ساختار استاندارد ISO/IEC 27034

استاندارد ISO/IEC 27034 شامل شش قسمت است. این قسمت از استانداردهای ISO/IEC 27034 مرور کلی و مفاهیم ضروری را ارائه می‌کند. این قسمت جامعیت داشته و برای ارزیابی نیاز پیاده‌سازی استاندارد ملی ISO/IEC 27034 در یک سازمان و نیز برای اهداف نمایش و آموزش کفایت می‌کند. این قسمت از استاندارد ISO/IEC 27034 به تنهایی برای پیاده‌سازی استاندارد ملی ISO/IEC 27034 کافی نیست.

استانداردهای 4, 3, 2-27034 ISO/IEC باید توسط سازمان‌هایی که تمایل دارند استاندارد ISO/IEC 27034 را پیاده‌سازی کنند کسب شده باشد. این قسمت‌ها شامل مباحث، شماره‌دهی، ساختارها و توصیف‌های عمیقی برای همه مفاهیم ارائه شده در این قسمت از استاندارد ISO/IEC 27034 می‌شوند.

استاندارد ISO/IEC 27034-5 به‌طور خاص برای سازمان‌هایی کارایی خواهد داشت که تمایل دارند با ایجاد یک ساختمان داده‌ی استاندارد و یک پروتکل استاندارد برای توزیع کنترل‌ها، کنترل‌ها را کسب کرده یا توزیع کنند. به‌عنوان مثال یک سازمان بزرگ ممکن است به توزیع خودکار و نیز به‌روزرسانی کنترل‌ها برای همه واحدهای زیرمجموعه خود تمایل داشته باشد.

استاندارد ISO/IEC 27034-5 مثال‌هایی از کنترل‌هایی برای نیازهای خاص امنیت برنامه کاربردی ارائه کرده و برای سازمان‌هایی کارایی خواهد داشت که تمایل دارند استاندارد ISO/IEC 27034 را پیاده‌سازی کنند یا سازمان‌هایی که تمایل دارند کنترل‌های خاصی را توسعه دهند.

محتوای این شش قسمت به شرح زیر است:

#### **قسمت ۱- مرور کلی و مفاهیم**

قسمت ۱ مرور کلی بر امنیت برنامه کاربردی ارائه می‌دهد. این قسمت به ارائه تعاریف، مفاهیم، اصول و فرایندهای مورد بحث در امنیت برنامه کاربردی می‌پردازد.

#### **قسمت ۲- چارچوب الزامی سازمان**

قسمت ۲ معرف بحثی عمیق در زمینه چارچوب الزامی سازمان، اجزای آن و فرایندهای سطح سازمانی برای مدیریت آن ارائه می‌دهد. این قسمت به توضیح روابط بین این فرایندها، فعالیت‌های مرتبط با آنها و وسایل و ابزارهایی می‌پردازد که از طریق آنها این فرایندها از فرایند مدیریت امنیت برنامه کاربردی حمایت می‌کنند. این قسمت در مورد این بحث می‌کند که چگونه یک سازمان باید استاندارد ISO/IEC 27034 را پیاده‌سازی کرده و آن را در فرایندهای موجود خود بگنجاند.

#### **قسمت ۳- فرایند مدیریت امنیت برنامه کاربردی**

قسمت ۳ معرف بحثی عمیق در زمینه فرایندهای مورد بحث در یک پروژه کاربردی است:

تعیین نیازها و محیط برنامه، ارزیابی مخاطرات امنیت برنامه کاربردی، ایجاد و نگهداری چارچوب الزامی برنامه کاربردی، تحقق و به‌کارگیری برنامه کاربردی و تأیید اعتبار امنیت آن در کل مدت چرخه حیات آن. این قسمت به توضیح روابط بین این فرایندها، فعالیت‌ها و وابستگی متقابل آنها می‌پردازد و توضیح می‌دهد که چگونه این فرایندها امنیت را در یک پروژه کاربردی ارائه می‌کنند.

#### **قسمت ۴- اعتبارسنجی امنیت برنامه کاربردی**

قسمت ۴ معرف بحثی عمیق در مورد اعتبارسنجی و فرایند گواهی امنیت برنامه کاربردی است که به اندازه‌گیری سطح اعتماد واقعی برنامه کاربردی پرداخته و آن را با سطح اعتماد هدف‌گذاری شده برنامه کاربردی که قبلاً توسط سازمان انتخاب شده، مقایسه می‌کند.

#### **قسمت ۵- پروتکل‌ها و ساختمان داده کنترل امنیت برنامه کاربردی**



قسمت ۵ معرف پروتکل‌ها و الگوی سامانه نشانه‌گذاری گسترده (XML) برای کنترل امنیت برنامه کاربردی بر مبنای مجموعه‌های استاندارد ISO/IEC-TS 15000 است: سامانه نشانه‌گذاری گسترده تجارت الکترونیک (ebXML). این قسمت به سازمان‌ها کمک خواهد کرد تا ساختار اطلاعات کنترل‌های امنیت برنامه کاربردی خود و سایر اجزای استاندارد ISO/IEC 27034 را تأیید اعتبار کنند و نیز به خودکار کردن توزیع، به‌روزرسانی و استفاده از کنترل‌های امنیت برنامه کاربردی کمک می‌کند.

#### قسمت ۶- راهنمای امنیتی برای برنامه‌های کاربردی ویژه

قسمت ۶ در صورت لزوم، می‌تواند مثال‌هایی از کنترل‌های امنیت برنامه کاربردی متناسب برای نیازهای خاص امنیت برنامه کاربردی ارائه دهد.

### ۶ مقدمه‌ای بر امنیت برنامه کاربردی

#### ۶-۱ کلیات

امنیت برنامه کاربردی فرایندی است که برای اعمال کنترل و سنجش برنامه‌های یک سازمان و به‌منظور مدیریت مخاطره‌ی استفاده از آنها، اجرا می‌شود. کنترل‌ها و سنجش‌ها می‌توانند بر خود برنامه کاربردی (فرآیندها، اجزا، نرم‌افزار و نتایج آن)، اطلاعات آن (داده‌های پیکربندی، داده‌های کاربری، داده‌های سازمانی) و نیز بر کل فناوری، فرایندها و کنشگرهای مورد بحث در چرخه حیات برنامه کاربردی اعمال شوند.

#### ۶-۲ امنیت برنامه کاربردی در برابر امنیت نرم‌افزار

یک برنامه کاربردی یک راه‌کار فناوری اطلاعات است که شامل نرم‌افزار می‌شود. (به بند ۳ رجوع کنید). لذا امنیت برنامه کاربردی مفهومی گسترده‌تر است که امنیت نرم‌افزار را شامل می‌شود.

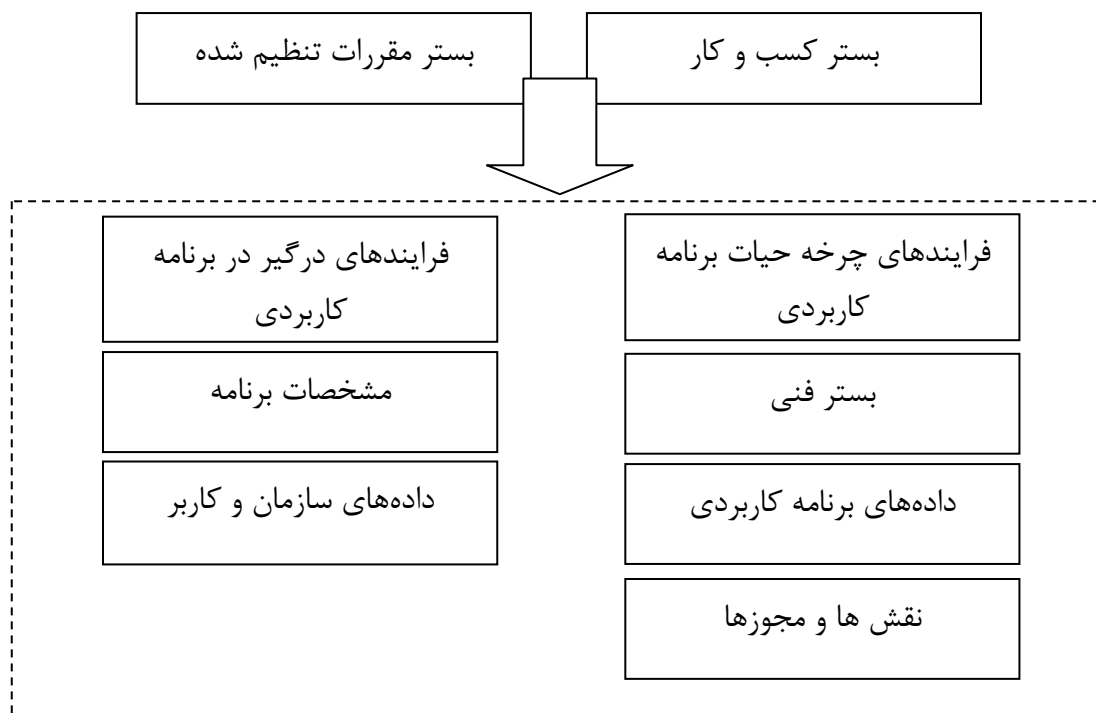
#### ۶-۳ محدوده امنیت برنامه کاربردی

#### ۶-۳-۱ کلیات

امنیت برنامه کاربردی از داده‌های حیاتی که توسط یک برنامه کاربردی متناسب با نیاز سازمان محاسبه، استفاده، ذخیره و منتقل شده‌اند، محافظت می‌کند. این پشتیبانی نه تنها دسترس‌پذیری، یکپارچگی و محرمانگی اطلاعات را تضمین می‌کند، بلکه تضمین‌کننده احراز هویت و انکارناپذیری کاربرانی است که به این اطلاعات دسترسی دارند. اهمیت و حساسیت اطلاعات و سایر سرمایه‌ها باید توسط سازمان در فرایند ارزیابی مخاطره امنیتی آن مشخص شده باشد.

داده‌های حیاتی مستلزم حفاظت، شامل کد منبع، کد دودویی و کد زمان اجرایی است که برنامه کاربردی طبق آن اجرا می‌شود.

شکل ۲ نمایش ترسیمی محدوده امنیت برنامه کاربردی است. این محدوده در شکل به صورت خط‌چین نشان داده شده است.



این نمایش ترسیمی به معنای آن نیست که همه عناصر موجود در محدوده بالا قسمتی از برنامه کاربردی هستند، بلکه بیشتر به این معنی است که همه این عناصر باید مورد حفاظت قرار گیرند تا امنیت برنامه کاربردی تضمین شود. بنابراین محدوده امنیت برنامه کاربردی گسترده‌تر از محدوده خود برنامه کاربردی است. جدول زیر این تفاوت را نشان می‌دهد.

جدول ۱- محدوده برنامه کاربردی در برابر محدوده امنیت برنامه کاربردی

عناصر مربوط	در محدوده برنامه کاربردی	در محدوده امنیت برنامه کاربردی
داده‌های سازمانی و کاربر (۹-۳-۶)		✓
داده‌های برنامه کاربردی (۸-۳-۶)	✓	✓
جایگاه‌ها و مجوزها (۱۰-۳-۶)	✓	✓
مشخصات برنامه کاربردی (۷-۳-۶)	✓	✓
زمینه فنی (۶-۳-۶)		✓
فرایندهای مورد بحث در برنامه کاربردی (۵-۳-۶)		✓
فرایندهای چرخه حیات برنامه کاربردی (۴-۳-۶)		✓
زمینه کسب و کار (۲-۳-۶)		✓
زمینه مقررات تنظیم شده (۳-۳-۶)		✓

داده‌ها و فرایندهای زیر در محدوده امنیت برنامه کاربردی قرار دارند و باید حفاظت شوند.

### ۶-۳-۲ زمینه کسب و کار

زمینه کسب و کار به همه امور، مقررات و قیود وابسته به کسب و کار مربوط می‌شود که از زمینه کسب و کار سازمان ریشه می‌گیرند.

### ۶-۳-۳ زمینه مقررات تنظیم‌شده

زمینه مقررات تنظیم‌شده به همه قوانین، مقررات و قواعد مشترکی مربوط می‌شود که از قلمرو یا زمینه قضایی نشأت گرفته و بر کارایی برنامه کاربردی یا بر استفاده برنامه کاربردی از اطلاعات تأثیر می‌گذارد. (مثل مخاطرات ناشی از قوانین ملی متفاوت در کشورهایی که یک برنامه کاربردی مشابه به کار گرفته خواهد شد).

### ۶-۳-۴ فرایندهای چرخه حیات برنامه کاربردی

همه فرایندهای سازمانی موجود یا لازم که در چرخه حیات برنامه کاربردی مورد بحث هستند، باید حفاظت شوند. مانند:

- الف) فرایندهای آموزشی، ممیزی و صلاحیتی؛
- ب) فرایندهای تحقق (توسعه، مدیریت پروژه، نگهداری، نسخه گذاری، آزمون و غیره)؛ و
- پ) فرایندهای عملیاتی.

### ۶-۳-۵ فرایندهای مورد بحث در برنامه کاربردی

همه فرایندهای سازمانی موجود یا لازم که تحت تأثیر مشخصات ضروری برنامه کاربردی و اطلاعات حیاتی هستند، باید مورد حفاظت قرار گیرند. مانند:

- الف) فرایندهای استفاده و مدیریت؛
- ب) فرایندهای نگهداری و پشتیبان‌گیری؛
- پ) فرایندهای توزیع و به کارگیری؛ و
- ت) فرایندهایی که تحت تأثیر برنامه کاربردی قرار می‌گیرند یا مورد نیاز آن هستند.

### ۶-۳-۶ زمینه فنی

تمامی مولفه‌های فنی و محصولاتی که از مشخصات حیاتی یا داده‌های حیاتی حمایت می‌کنند، باید حفظ شوند. مانند:

- الف) پایانه، شبکه ارتباطی و سایر محیط‌های مجاز؛
- ب) سیستم عامل، پیکربندی و خدمات؛
- پ) پیوندها و درگاه‌های مجاز ارتباطی،
- ت) نرم‌افزارهای تجاری و عمومی و سایر محصولات مانند سامانه‌های مدیریتی پایگاه داده که توسط برنامه و زیرساخت فنی آن به کار می‌روند؛
- ث) صلاحیت و سایر فرایندهای مرتبط با زمینه فنی؛ و
- ج) محصولاتی که تحت تأثیر یا مورد استفاده برنامه کاربردی قرار می‌گیرند.

### ۶-۳-۷ مشخصات برنامه کاربردی

همه خصوصیات برنامه کاربردی باید در برابر تغییرات غیرمجاز حفاظت شوند. مانند:

الف) مشخصات سخت‌افزاری؛

ب) مشخصات امنیتی؛

پ) کارکردهای برنامه کاربردی؛

ت) مشخصات پایانه مشتری؛ و

ث) مشخصات دفتر پشتیبانی.

### ۶-۳-۸ اطلاعات برنامه کاربردی

همه اطلاعات برنامه کاربردی باید حفاظت شوند. مانند:

الف) داده‌های پیکربندی برنامه کاربردی؛

ب) آیین‌نامه مضاعف برنامه کاربردی

پ) آیین‌نامه منبع برنامه کاربردی

ت) اجزای برنامه‌ای و کتابخانه‌ای؛ و

ث) اسناد کاربردی اجزا و کارکردهای حیاتی.

### ۶-۳-۹ داده‌های سازمانی و کاربری

همه اطلاعات حیاتی سازمان و کاربر باید حفاظت شوند. مانند:

الف) گواهی‌ها؛

ب) کلیدهای محرمانه؛

پ) اطلاعات حیاتی - مأموریتی؛

ت) اطلاعات شخصی؛ و

ث) اطلاعات پیکربندی کاربر.

### ۶-۳-۱۰ نقش‌ها و مجوزها

همه اطلاعات حیاتی مدیریت هویت و مجوزها باید حفاظت شوند. مانند:

الف) اطلاعات مدیریت هویت؛

ب) اطلاعات شناسایی و احراز هویت و

پ) اطلاعات اختیارات.

### ۶-۴ نیازهای امنیت برنامه کاربردی

#### ۶-۴-۱ منابع نیازهای امنیت برنامه کاربردی

همان‌طور که در استاندارد ملی ایران به شماره ۲۷۰۰۵ بحث شد، نیازهای امنیت برنامه کاربردی توسط ارزیابی مخاطره و برطرف‌سازی مخاطره شناخته می‌شوند و توسط عواملی چون مشخصات برنامه، محیط

هدف‌گذاری شده برنامه (زمینه کسب و کار، مقررات تنظیم‌شده و فنی) داده‌های حیاتی و تصمیمات مالک برنامه کاربردی اداره می‌شوند.

نیازهای امنیتی کارکردی مشخص می‌کند که کدام کارکردهای امنیتی در برنامه کاربردی پیاده‌سازی خواهند شد. نیازهای امنیتی غیر کارکردی به آن دسته از ویژگی‌های امنیتی مربوط می‌شوند که برنامه کاربردی باید ارائه دهد. این کنترل‌ها باید قبلاً توسط سازمان به‌طور کامل تعیین و تصویب شده باشند.

#### ۶-۴-۲ مهندسی نیازهای امنیت برنامه کاربردی

مهندسی نیازهای برنامه کاربردی فرایند گسترده‌تری بر مبنای گردآوری، تحلیل و تعیین نیازها برای یک برنامه کاربردی است. این فرایند باید با ارزیابی مخاطره افزایش یابد تا با نیازهای امنیتی یکی شود. ارزیابی مخاطره مانند هر نیاز دیگری باید شامل استفاده از روش‌های اجرایی تکرارپذیر و نظام‌مند شود که تضمین می‌کنند مجموعه نیازهای حاصل برای مالک برنامه کاربردی، کامل، سازگار، قابل فهم و تحلیل‌پذیر است. همچنین نیازها و در نتیجه دست‌یابی باید قابل سنجش باشند.

#### ۶-۴-۳ ISMS

#### ۶-۴-۳-۱ ISMS سازمانی

همه اطلاعاتی که توسط یک سازمان حفظ و پردازش شده است در معرض مخاطراتی همچون خطا، سیل، آتش‌سوزی، سرقت و غیره و نیز در معرض مخاطرات مربوط به فناوری مورد استفاده قرار دارد. اصطلاح «امنیت اطلاعات» بر اطلاعات به‌عنوان یک سرمایه با ارزش اطلاق می‌شود که مستلزم حفاظتی مناسب و درخور است. بر اساس استاندارد ملی ایران به شماره ۲۷۰۰۰، ISMS مدلی برای برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و اصلاح حفاظت از دارایی‌های اطلاعاتی یک سازمان بر مبنای دیدگاه مخاطره کسب و کار را فراهم می‌کند. حفاظت از ارزیابی اطلاعات یک سازمان باید با مخاطرات مربوطه و سطوح پذیرش کسب و کار در یک سطح قرار گیرد. این مدیریت مخاطرات، بر امنیت اطلاعات تکیه کرده و انواع مخاطرات مربوط به انواع اطلاعات سازمان را پوشش می‌دهد.

#### ۶-۴-۳-۲ امنیت برنامه کاربردی در زمینه ISMS

امنیت برنامه کاربردی با ایجاد مدلی برای برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و اصلاح حفاظت از ارزیابی اطلاعات مرتبط با برنامه‌های کاربردی یک سازمان، از اهداف ISMS در سطح سازمان پشتیبانی می‌کند. امنیت برنامه کاربردی باید کنترل‌های متناسب و مدارکی فراهم کند تا به مدیران سازمان ثابت کند که مخاطرات مورد بحث در به‌کارگیری یک برنامه کاربردی به درستی مدیریت شده‌اند. ISMS با تضمین این که همه مخاطرات مربوط به اطلاعات سازمانی از جمله اطلاعات در دسترس برنامه‌ها، مدیریت شده‌اند، بر امنیت برنامه کاربردی حاکم است. کنترل‌های مورد نیاز سامانه مدیریت امنیت اطلاعات تا سطح برنامه کاهش یافته‌اند.

## ۵-۶ مخاطره

### ۱-۵-۶ مخاطره امنیت برنامه کاربردی

مخاطره‌ای که به دنبال به کارگیری یک برنامه کاربردی خاص برای یک سازمان مطرح می‌شود. مخاطره امنیت برنامه کاربردی از موارد زیر ناشی می‌شود:

الف) تهدیداتی که اطلاعات در دسترس یک برنامه کاربردی را مورد هدف قرار می‌دهند؛  
ب) آسیب‌پذیری‌ها؛ و

پ) تأثیر سواستفاده موفقیت‌آمیز تهدیدها از آسیب‌پذیری‌ها.

فعالیت‌های تعیین، پیگیری، ذخیره، سنجش و گزارش مخاطرات برنامه کاربردی بیشترین اهمیت را دارند. نیازهای امنیت برنامه کاربردی و کنترل‌های مورد نیاز برای پاسخگویی به آنها یکی از واکنش‌های این مخاطره است. فرایند ارزیابی مخاطره امنیت برنامه کاربردی مورد نیاز است زیرا مخاطره در طی زمان تغییر می‌کند و در نتیجه تشخیص و ذخیره مداوم و سازگار اطلاعات مخاطره مورد نیاز است.

### ۲-۵-۶ آسیب‌پذیری‌های برنامه کاربردی

آسیب‌پذیری‌ها نتیجه کنترل‌های ناکافی یا ناموجود هستند. آسیب‌پذیری‌هایی که نتیجه کنترل نامناسب هستند منجر به مخاطره غیر قابل قبول برنامه کاربردی می‌شوند.

آسیب‌پذیری‌ها ناشی از موارد زیر هستند:

الف) کنشگران مانند برنامه‌نویسانی که کد ضعیف می‌نویسند، کاربرانی که حین استفاده از برنامه کاربردی خطا می‌کنند، تکنسین‌ها و تدوین‌گرانی که حین نگهداری برنامه کاربردی خطا می‌کنند؛

ب) فرایندهایی مانند رویه ای نامناسب آزمایش، مدیریت ضعیف پروژه، تمرکز ناکافی بر امنیت در کل فرایندهای چرخه حیات، اثرات متقابل پیش‌بینی نشده بین برنامه‌های کاربردی، کاربران و اپراتورها، فرایندهای نامناسب مدیریت تغییرات؛

پ) زمینه فنی، مانند انتخاب‌های بد زیرساخت فنی یا محصولات؛ و

ت) مشخصات، مانند طراحی نامناسب، آسیب‌پذیری‌های ناشی از اثرات متقابل سامانه یا خطا در واسطه‌های اجزا.

### ۳-۵-۶ تهدیدهای برنامه‌های کاربردی

یک تهدید این قابلیت را دارد که به اطلاعات حیاتی در محدوده برنامه کاربردی و در نتیجه به خود سازمان آسیب بزند. تهدیدات ناشی از موارد زیر هستند:

الف) محیط برنامه کاربردی: زمینه مقررات تنظیم‌شده، زمینه کسب و کار و زمینه فنی؛ و  
ب) کنشگران.

### ۴-۵-۶ اثر وارده بر برنامه‌های کاربردی

هزینه‌ای که یک سازمان به علت نقض دسترسی، صحت یا محرمانگی داده‌های حیاتی برنامه کاربردی متحمل می‌شود.

#### ۵-۵-۶ مدیریت مخاطره

مدیریت مخاطره امنیت برنامه کاربردی، فرایند نگهداری مخاطرات امنیت برنامه کاربردی در محدوده سطوح قابل قبول است. این مدیریت از طریق برطرف سازی مخاطرات غیر قابل قبول امنیت برنامه و به ویژه از طریق اعمال کنترل بر این مخاطرات حاصل شده است.

مدیریت مخاطره یک مفهوم کلیدی در امنیت اطلاعات است. بر اساس استاندارد ملی ایران به شماره ۲۷۰۰۵، «فرایند مدیریت مخاطره امنیت اطلاعات می تواند برای سازمان به عنوان یک کلیت، یا برای هر قسمت مجزای سازمان (مانند یک دپارتمان، یک مکان فیزیکی، یک خدمت)، یا برای هر سامانه اطلاعاتی موجود یا طراحی شده یا ابعاد خاصی از کنترل (مانند طرح ریزی مداوم کسب و کار) به کار رود.»

فرایند مدیریت مخاطره امنیت اطلاعات که در استاندارد ملی ایران به شماره ۲۷۰۰۵ ارائه شده مبتنی بر استقرار زمینه، ارزیابی مخاطره، برطرف سازی مخاطره، پذیرش مخاطره، اطلاع رسانی مخاطره، پایش و بازنگری مخاطره است.

یک فرایند مدیریت مخاطره امنیت برنامه کاربردی باید از عناصر فرآیندی مشابه با اجزای ظریف تر و هدفی سازگار با سطح برنامه کاربردی استفاده کند.

#### ۶-۶ هزینه های امنیت

هزینه اجرا، نگهداری و درستی سنجی کنترل های امنیتی برای یک سازمان باید بعد از بررسی مناسب مخاطرات و اثرات مرتبط با به کارگیری یک برنامه کاربردی، تا یک سطح قابل قبول (یا قابل تحمل) کاهش یابد. هزینه امنیت باید فشار بالقوه تهدیدات و آسیب پذیری ها را مورد محاسبه قرار دهد.

#### ۶-۷ محیط هدف

محیط هدف شامل زمینه مقررات تنظیم شده، کسب و کار و فنی است که سازمان در درون آن از برنامه کاربردی استفاده می کند. همه تهدیداتی که ممکن است به برنامه کاربردی آسیب بزنند ناشی از محیط آن هستند. به این دلیل، محیط هدف برنامه کاربردی باید به طور واضح در آغاز یک پروژه برنامه کاربردی تعریف شده باشد.

به منظور توسعه موفق و امن برنامه کاربردی، زمینه فنی سازمان باید با نیازهای محیط هدف برنامه موافقت کند. به محض اینکه برنامه کاربردی پیاده سازی شد، زمینه فنی سازمان می بایست محصولات و سخت افزار جدیدی را اضافه کند که بتوانند بر امنیت سایر برنامه های کاربردی اثر گذاشته و مخاطرات امنیت سازمان را تحت تأثیر قرار دهند.

از آنجا که مخاطره استفاده از برنامه کاربردی برای سازمان به محیط هدف برنامه مربوط می شود، نیازهای امنیتی جدید برنامه کاربردی می بایست به گونه ای تعریف شوند که این مخاطره های جدید را مدنظر قرار داده و کنترل هایی را انتخاب کنند که این گونه مخاطره ها را به حد قابل قبول (یا قابل تحمل) کاهش می دهند. این چنین کنترل های امنیتی را می توان وارد فرآیندهای چرخه حیات برنامه کاربردی کرد (مانند فرایند اکتساب یا فرایند امحا)، به کد منبع برنامه اضافه کرد یا بنا به نیاز سازمان در جایی از چرخه حیات برنامه کاربردی (۸-۳-۴) ادغام کرد.

## ۸-۶ کنترل ها و اهداف آنها

همان گونه که در استاندارد ملی ایران به شماره ۲۷۰۰۱ تعیین شده، کنترل ها و اهداف آنها می بایست جهت تأمین نیازهایی انتخاب و پیاده سازی شوند که توسط فرآیندهای ارزیابی مخاطره و مقابله با مخاطره تعیین می شوند. در مبحث امنیت برنامه کاربردی، فرآیند ارزیابی مخاطره، اهداف کنترل را براساس نیازهای امنیتی تعریف شده برنامه کاربردی تعیین می کند.

## ۷ فرآیندهای کلی این استاندارد ملی

### ۱-۷ اجزا، فرآیندها و چارچوبها

این استاندارد ملی اجزا، فرآیندها و چارچوبی برای کمک به سازمان ها جهت اکتساب، اجرا و استفاده از برنامه های کاربردی قابل اطمینان و با زیان امنیتی قابل قبول (یا قابل تحمل)، ارائه می کند. به طور دقیق تر، این اجزا، فرآیندها و چارچوبها مستندات قابل صحت سنجی از اینکه برنامه های کاربردی به سطح مورد نظر از اطمینان رسیده و در همان سطح باقی مانده اند را ارائه می کند.

تمام اجزا، فرآیندها و چارچوبها قسمتی از دو فرآیند کلی هستند که در شکل ۳ نیز نمایش داده شده اند:

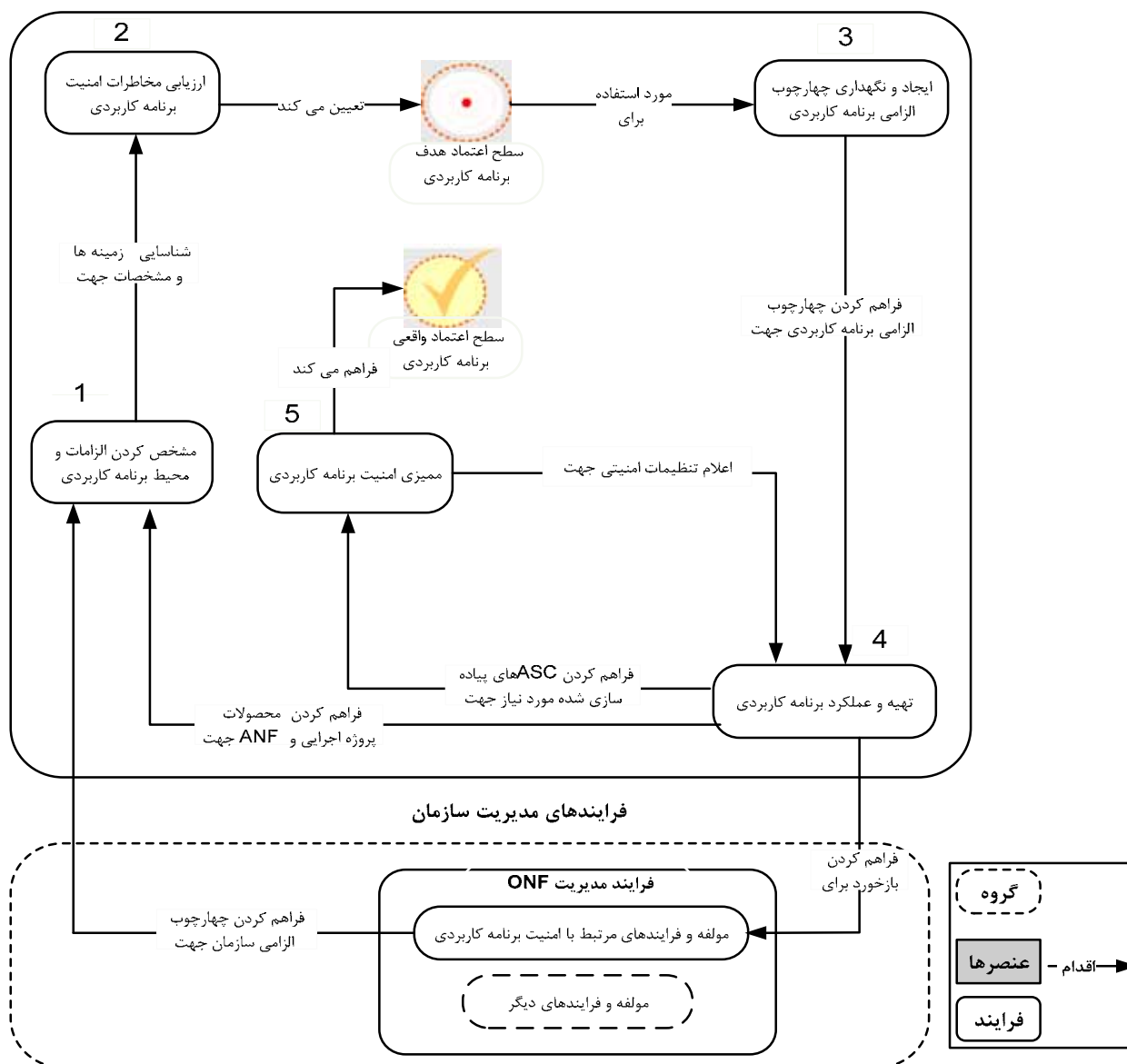
الف) فرآیند مدیریت ONF

ب) فرآیند ASMP

این دو در سطح و بازه های زمانی متفاوتی در سازمان مورد استفاده قرار گرفته و محدوده های متفاوتی نیز دارند. «فرآیند مدیریت ONF» فرایندی مستمر در سطح سازمان است و «ASMP» جهت مدیریت امنیت در پروژه برنامه های کاربردی خاص استفاده می شود.



### فرایندهای مدیریت امنیت برنامه کاربردی



شکل ۳ - فرایندهای مدیریت سازمان

### ۲-۷ فرآیند مدیریت ONF

این فرآیند باید جهت مدیریت جنبه‌هایی از ONF (چارچوب الزامی سازمان، به زیربند ۸-۱ مراجعه شود). استفاده شوند که مرتبط با امنیت برنامه کاربردی است. این چارچوب شامل کلیه فرایندهای موجود در امنیت برنامه کاربردی و همچنین مقررات، قوانین، بهترین عملکردها، نقش‌ها و مسئولیت‌پذیری‌های مورد قبول سازمان است. این فرآیند تمامی زمینه‌های سازمان را تعریف کرده و مرجع منحصربه‌فرد امنیت برنامه کاربردی درون سازمان می‌شود.

**یادآوری ۱-** سازمان معمولاً چارچوب الزامی را جهت اهداف دیگری خارج از دامنه این استاندارد ملی به کار می‌گیرد و معمولاً فرآیندهایی نیز به منظور مدیریت آن تعریف می‌کند. بنابراین ONF و فرآیندهای مدیریتی مربوط به آن از دیدگاه تأمین اهداف این استاندارد ملی، زیرمجموعه‌ای از یک ONF موجود و فرآیندهای مربوطه است.

فرآیندهای مرتبط با امنیت برنامه کاربردی باید قسمتی از ONF باشند. براساس این استاندارد ملی، نظارت و مسئولیت نگهداری و تأیید عوامل ONF مربوط به امنیت برنامه کاربردی باید به عهده نقشی سازمانی گذاشته شود که این استاندارد ملی آن را «کمیتة ONF» می‌نامد.

**یادآوری ۲-** فرآیند مدیریت ONF و اجزای مربوطه و فرآیندهای زیرمجموعه با جزئیات بیشتر در زیربند ۸-۱-۳-۲ و همچنین در استاندارد ISO/IEC 27034-2 آمده است.

## **۷-۳ فرایند مدیریت امنیت برنامه کاربردی**

### **۷-۳-۱ کلیات**

فرایند مدیریت امنیت برنامه کاربردی فرایند کلی مدیریت امنیت برای کلیه برنامه‌های کاربردی مورد استفاده یک سازمان است. پیوست پ نشان می‌دهد که ASMP نمونه تخصصی‌شده فرایند مدیریت مخاطره استاندارد ملی ایران به شماره ۲۷۰۰۵ است.

فرایند مدیریت امنیت برنامه کاربردی در پنج مرحله اجرا می‌شود:

(الف) مشخص کردن نیازها و محیط برنامه کاربردی

(ب) ارزیابی مخاطرات امنیتی برنامه کاربردی

(ج) ایجاد و نگهداری چارچوب الزامی برنامه کاربردی

(د) تهیه و اجرای برنامه کاربردی

(ه) ممیزی امنیت برنامه کاربردی

**یادآوری - ASMP** به تفصیل در بند ۸ و در استاندارد ISO/IEC 27034-3 آمده است.

### **۷-۳-۲ مشخص کردن نیازها و محیط برنامه کاربردی**

قدم اول ASMP مشخص کردن تمام نیازهای برنامه کاربردی به شرح زیر است:

(الف) کنشگرها

(ب) مشخصات

(پ) اطلاعات

(ت) محیط

محیط برنامه کاربردی شامل این موارد است:

(الف) زمینه زمینه فنی

(ب) زمینه کسب و کار

(پ) زمینه مقررات تنظیم‌شده

یادآوری: زمینه به تفصیل در زیربندهای ۱-۲-۸ و ۲-۲-۱-۸ ارائه شده است. این قدم مربوط به مرحله تأسیس زمینه در فرایند مدیریت مخاطره می‌شود که توسط استاندارد ملی ایران به شماره ۲۷۰۰۵ تعیین شده و اطلاعات لازم جهت قدم بعدی ارزیابی مخاطره را فراهم می‌کند.

#### ۷-۳-۳ ارزیابی مخاطرات امنیت برنامه کاربردی

قدم دوم ASMP فرایندی مطابق با ارزیابی مخاطره و قسمتی از مرحله برطرف‌سازی مخاطره در فرایند مدیریت مخاطره‌ای است که در استاندارد ملی ایران به شماره ۲۷۰۰۵، ولی با سطح تفکیک بهتر و محدوده عمل محدود به یک پروژه برنامه کاربردی خاص آمده است.

ارزیابی مخاطره شامل شناسایی مخاطره، تحلیل مخاطره و سنجش مخاطره است. این مرحله از ASMP نیازمندی‌های امنیتی را فراهم می‌کنند که برای کسب سطح اعتماد مطلوب یک برنامه کاربردی مورد استفاده قرار می‌گیرند. این موضوع سطح اعتماد هدف‌گذاری شده نام دارد و باید مورد تأیید مالک برنامه کاربردی قرار گیرد.

به همین دلیل این مرحله با قسمت انتخاب روش برطرف‌سازی مخاطره مرحله برطرف‌سازی مخاطره فرایند مدیریت مخاطره در استاندارد ملی ۲۷۰۰۵ مطابقت دارد.

#### ۷-۳-۴ ایجاد و نگهداری چارچوب الزامی برنامه

مرحله سوم ASMP، تمام عناصر مرتبط ONF قابل اعمال بر یک پروژه کاربردی خاص را انتخاب می‌کند. نتیجه آن چارچوب الزامی برنامه کاربردی (ANF) خواهد بود. سطح اعتماد هدف‌گذاری شده برنامه کاربردی، زمینه‌های برنامه کاربردی (مقررات تنظیم‌شده، کسب و کار یا فنی)، مسئولیت‌پذیری‌ها و قابلیت‌های حرفه‌ای کنشگرها و خصوصیات برنامه کاربردی، محتوای دقیق ANF را تعیین می‌کنند.

همچنین در این مرحله است که سازمان چرخه حیات برنامه کاربردی، شامل فعالیت‌های مورد نیاز پروژه حاضر را تعیین می‌کند. به‌عنوان مثال یک پروژه درون سازمانی نیاز به فعالیت‌های برون‌سپاری ندارد. در مجموع، سازمان کنترل‌های امنیت برنامه کاربردی قابل اجرا برای پروژه برنامه کاربردی را انتخاب می‌کند. این مرحله مطابق قسمت «آماده‌سازی و پیاده‌سازی برنامه‌های برطرف‌سازی مخاطره» است که خود قسمتی از مرحله «برطرف‌سازی مخاطره» در فرایند مدیریت مخاطره تعیین‌شده در استاندارد ملی ۲۷۰۰۵ است.

یادآوری- این مرحله از ASMP و اجزا و فرایندهای مربوطه با جزئیات بیشتر در زیربند ۸-۳ ارائه شده است.

#### ۷-۳-۵ تأمین و بهره‌برداری از برنامه کاربردی

مرحله چهارم ASMP استفاده واقعی از «کنترل‌های امنیتی برنامه کاربردی»، مطابق آن چه که توسط ANF در چرخه حیات برنامه کاربردی ارائه شده است. گروه پروژه، کنترل‌های امنیت برنامه کاربردی را تحت چارچوب الزامی سازمان، در دو مرحله پیاده‌سازی می‌کنند:

الف) قسمت فعالیت امنیتی هر ASC توسط کنشگر تعیین‌شده در ASC انجام می‌پذیرد.

ب) قسمت سنجش امنیت هر ASC توسط کنشگر تعیین‌شده در ASC انجام می‌پذیرد.

مرحله چهارم مطابق قسمت «طرح‌های آماده سازی و پیاده‌سازی برنامه‌های برطرف‌سازی مخاطره» است که خود قسمتی از مرحله «برطرف‌سازی مخاطره» در فرآیند مدیریت مخاطره تعیین‌شده در استاندارد ملی ایران به شماره ۲۷۰۰۵ است.

**یادآوری-** این مرحله از ASMP و اجزا و فرایندهای مربوط با جزئیات بیشتر در زیربند ۸-۴ ارائه شده است.

### ۷-۳-۶ ممیزی امنیت برنامه کاربردی

پنجمین و آخرین مرحله ASMP ممیزی امنیت برنامه کاربردی است. در این مرحله، گروه درستی‌سنجی، اجرای تمامی راه‌کارهای درستی‌سنجی ارائه شده توسط ASCها در چارچوب الزامی برنامه کاربردی و دستیابی به نتایج مورد نظر را می‌سجد. این مرحله مطابق مرحله «نظارت و بازبینی» فرایند مدیریت مخاطره تعیین‌شده در استاندارد ملی ایران به شماره ۲۷۰۰۵ است.

**یادآوری-** این مرحله از ASMP و اجرا و فرایندهای مربوط با جزئیات بیشتر در زیربند ۸-۵ ارائه شده است.

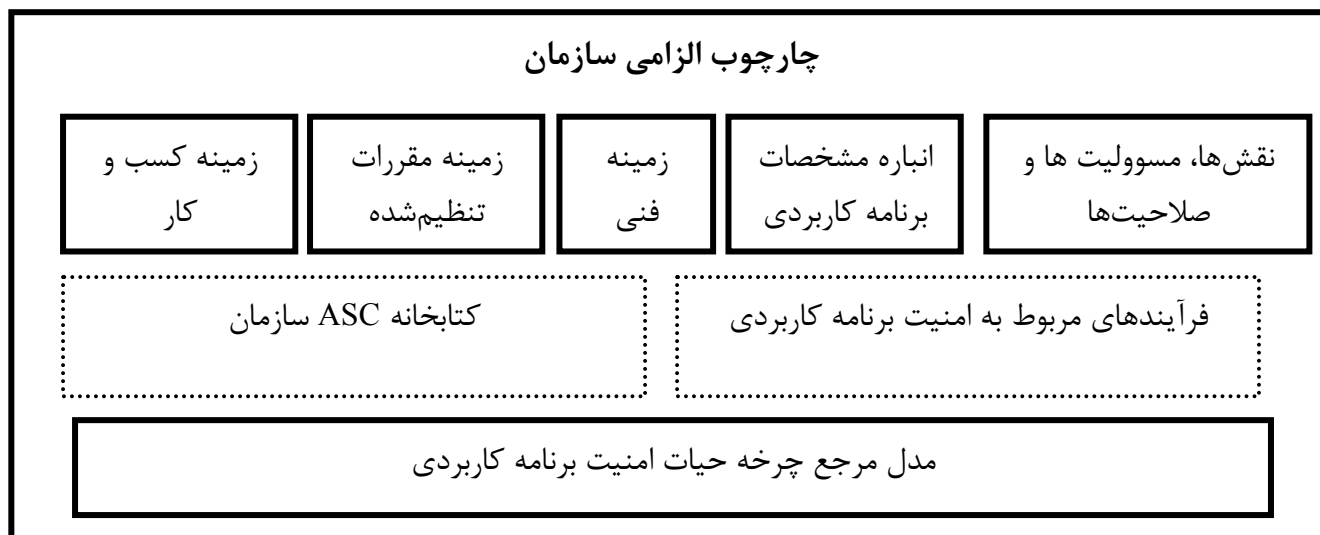
## ۸ مفاهیم

### ۸-۱ چارچوب الزامی سازمان

#### ۸-۱-۱ کلیات

چارچوب الزامی سازمان (ONF) چارچوبی است که در آن بهترین روش‌های امنیت برنامه کاربردی از نظر سازمان مربوطه ذخیره شده یا بهترین روش‌های امنیت برنامه از آن بازیافت یا استخراج می‌شوند. این چارچوب اجزای ضروری، فرایندهایی که این اجزا را مورد استفاده قرار می‌دهند و فرایندهای مدیریت ONF را شامل می‌شود. ONF زیرساخت امنیت برنامه کاربردی در یک سازمان است و تمام تصمیمات امنیت برنامه کاربردی در یک سازمان براساس آن اتخاذ می‌شوند. به‌عنوان مثال، اگر راهنماهای کدگذاری در ONF موجود باشند، فعالیت بازنگری کد به‌عنوان کنترل امنیت برنامه کاربردی اجباری اعمال می‌شود. همان‌گونه که در شکل ۳ مشاهده می‌شود، ONF ورودی اصلی ASMP است که برای هر پروژه برنامه کاربردی در سازمان اجرا می‌شود.

شکل ۴، شمای کلی از محتویات ONF را نمایش می‌دهد.



#### شکل ۴- چارچوب الزامی سازمان (ساده شده)

به منظور پرداختن صحیح به نگرانی‌های امنیت برنامه کاربردی، یک سازمان باید ONF رسمی شامل اجزای زیر را داشته باشد:

- الف) زمینه کسب و کار
  - ب) زمینه مقررات تنظیم شده
  - پ) زمینه‌های فنی
  - ت) انباره مشخصات برنامه کاربردی
  - ث) نقش‌ها، مسئولیت‌پذیری‌ها و صلاحیت‌ها
  - ج) کتابخانه ASC سازمان
  - چ) فرآیندهای مربوط به امنیت برنامه کاربردی
  - ح) مدل مرجع چرخه حیات امنیت برنامه کاربردی
- ONF رسمی باید شامل فرآیندهای زیر نیز باشد:
- الف) فرآیند مدیریت ONF
  - ب) زیرفرآیندهای مدیریت ONF

#### ۸-۱-۲ اجزا

##### ۸-۱-۲-۱ زمینه کسب و کار

زمینه کسب و کار تمام استانداردها و بهترین روش‌های به کار گرفته شده توسط سازمان را که می‌توانند بر پروژه‌های کاربردی تأثیرگذار باشند را فهرست و ثبت می‌کند.

زمینه کسب و کار شامل موارد زیر می‌شود:

- الف) فرآیندهای مدیریت پروژه، توسعه، تحلیل مخاطره، عملیات، ممیزی و کنترل
- ب) سیاست امنیتی سازمان
- پ) روش‌های زمینه کسب و کار
- ت) روش توسعه استفاده شده توسط سازمان
- ث) بهترین روش‌ها در مورد کلیه زبان‌های برنامه‌نویسی استفاده شده توسط سازمان و فهرست شده در زمینه فنی.
- ج) فرایند مدیریت پروژه رسمی سازمان
- چ) اقتباس سایر استانداردهای ISO/IEC مرتبط مانند استاندارد ملی ایران به شماره ۲۷۰۰۱، استاندارد ملی ایران به شماره ۲۷۰۰۲ و استاندارد ISO/IEC 5288.

#### ۸-۱-۲-۲ زمینه مقررات تنظیم شده

زمینه نظارتی هرگونه قانون و مقررات را که می‌تواند بر پروژه‌های کاربردی تأثیر بگذارد، در هر محلی که سازمان به فعالیت مشغول است را ثبت و فهرست می‌کند. این امر شامل قوانین، قواعد و مقررات مربوط به کشور یا زمینه قانونی می‌گردد که برنامه در آنجا توسعه و یا پخش و یا استفاده می‌شود. سازمانی که برنامه کاربردی مشابهی را در بیش از یک کشور توزیع یا استفاده می‌کند ممکن است ملزم به پاسخگویی به اقدامات امنیتی متفاوت هر کشور شود.

#### ۸-۱-۲-۳ انباره مشخصات برنامه کاربردی

انباره مشخصات برنامه کاربردی، الزامات کارکرد عمومی فناوری اطلاعات سازمان را همراه با راه‌حل‌های از پیش تعیین شده ثبت و فهرست می‌کند. خصوصیات برنامه کاربردی باید شامل موارد زیر باشد:

الف) مشخصاتی درباره چگونگی انجام محاسبات، ذخیره داده‌ها و انتقال آنها توسط برنامه کاربردی

ب) پارامترها، کارکردها، خدمات و الزامات معمول برنامه کاربردی

پ) کد منبع، کد دو دویی، کتابخانه و محصولات و خدماتی که برنامه کاربردی آنها را استفاده یا بر آنها تکیه می‌کند.

مشخصات اضافه ممکن است شامل جزئیات نحوه تعامل برنامه با موارد زیر باشد:

الف) سامانه‌های دیگر

ب) زیرساخت زمان اجرا که برنامه کاربردی به آن متکی است

پ) فهرست کنترل‌های موجود در محیط زمان اجرای برنامه کاربردی

#### ۸-۱-۲-۴ زمینه فنی

زمینه فنی از انباره کلیه محصولات، خدمات و فناوری‌های فناوری اطلاعات تشکیل شده که برای پروژه‌های برنامه کاربردی در دسترس سازمان هستند. این محصولات، خدمات و فناوری‌ها تهدیدهایی که برنامه در معرض آنها قرار دارد را مشخص می‌کند. زمینه فنی شامل رایانه‌ها، ابزارها، محصولات و خدمات فناوری اطلاعات، زیرساخت ارتباطات و سایر وسایل فنی است.

مثال ۱- زمینه‌های فناوری که ممکن است تأثیری بر امنیت برنامه کاربردی داشته باشند، زیرساخت سرویس‌دهنده/مشری، زیرساخت وب، زیرساخت شبکه، محیط و ابزارهای توسعه را شامل می‌شوند.

زمینه فنی همچنین امکان معرفی کنترل‌های امنیت برنامه کاربردی خاص را در برنامه کاربردی مشخص می‌کند.

مثال ۲- اگر زمینه فنی شامل مکانیزم احراز هویت TLS1.0 جهت پشتیبانی از کارکرد احراز هویت دوسویه نباشد، ممکن است برنامه کاربردی شامل ASC مبتنی بر TLS1.0 نباشد. اگر این کارکرد در سطح اعتماد هدف‌گذاری شده برنامه کاربردی مورد نیاز باشد، گروه پروژه باید ASC جایگزینی را برای دستیابی به کارکرد احراز هویت دوسویه انتخاب کند.

زمینه فنی باید شامل موارد زیر باشد:

الف- فناوری‌های موجود جهت پروژه‌های برنامه کاربردی سازمان

این انبار فناوری باید به صورت مداوم توسط کمیته ONF سازمان و از طریق بازخورد پروژه‌های برنامه کاربردی پیشین به‌روزرسانی شود.

ب- فناوری مورد نیاز برنامه کاربردی؛

فهرست فناوری‌های جدید از الزامات کارکردی جدید مشخص شده در جریان برنامه‌ریزی اغوایی پروژه برنامه کاربردی سرچشمه می‌گیرند. چنین الزاماتی باید به ONF اضافه شوند و یک فرایند سازمانی می‌بایست از این امر اطمینان حاصل کند که خصوصیات امنیتی فناوری‌های خاص جهت برآوردن الزامات جدید، قبل از تأیید، جهت قرار گرفتن در انبار فناوری‌های سازمان درک و ثبت شده‌اند؛ و

پ- فناوری‌های در دسترس؛

این مورد حاصل تحقیق، تحلیل رویه و نظارت بر فناوری است.

#### ۸-۱-۲-۵ جایگاه‌ها، مسئولیت‌پذیری‌ها و صلاحیت‌ها

ONF باید شامل موارد زیر باشد:

الف- فهرست‌ها و توصیف تمام جایگاه‌ها، مسئولیت‌پذیری‌ها و صلاحیت‌ها و صلاحیت‌های حرفه‌ای موردنیاز کنش‌گرهای درگیر در ایجاد و نگهداری و/یا جایگاه‌های ایجاد و نگهداری ASCها؛ و

ب- فهرست‌ها و توصیف تمام جایگاه‌ها، مسئولیت‌پذیری‌ها و صلاحیت‌ها و صلاحیت‌های حرفه‌ای موردنیاز کنش‌گرهای درگیر در چرخه حیات برنامه کاربردی سازمان از جمله: مدیران امنیت اطلاعات، مدیران پروژه، سرپرست‌ها، به‌دست‌آورنده‌های نرم‌افزار، مدیران توسعه نرم‌افزار، مالکان برنامه کاربردی، مدیران کاربری، مهندسين معمار، تحلیل‌گران، برنامه‌نویسان، آزمایش‌ده‌ها، سرپرست‌های سامانه، سرپرست‌های پایگاه داده‌ها، سرپرست‌های شبکه و کارکنان فنی.

این یک سیاست جامع سازمانی است که کمک می‌کند تا از اینکه تمام جایگاه‌های حیاتی فرایندها پر شده‌اند، تمام مسئولیت‌پذیری‌ها تعریف شده‌اند، از تضاد منافع جلوگیری شده‌است و تمام افرادی که جایگاه‌ها را پر کرده‌اند صلاحیت‌های حرفه‌ای کافی را دارند، اطمینان حاصل شود.

#### ۸-۱-۲-۶ کتابخانه ASC سازمان

##### ۸-۱-۲-۶-۱ کلیات

سازمان باید حداقل یک کتابخانه از کنترل‌های امنیت برنامه کاربردی تعریف کند. این کتابخانه، کتابخانه کنترل‌های امنیت برنامه کاربردی (کتابخانه ASC) نامیده می‌شود. این کتابخانه تمام ASCهای شناخته‌شده در سازمان را فهرست و ثبت می‌کند. این ASCها از استانداردها، بهترین تجربه‌ها و نقش‌ها، مسئولیت‌پذیری‌ها، جایگاه‌ها، صلاحیت‌های حرفه‌ای، زمینه‌های فنی، کسب و کار و مقررات تنظیم‌شده و مشخصات برنامه کاربردی استنتاج شده‌اند.

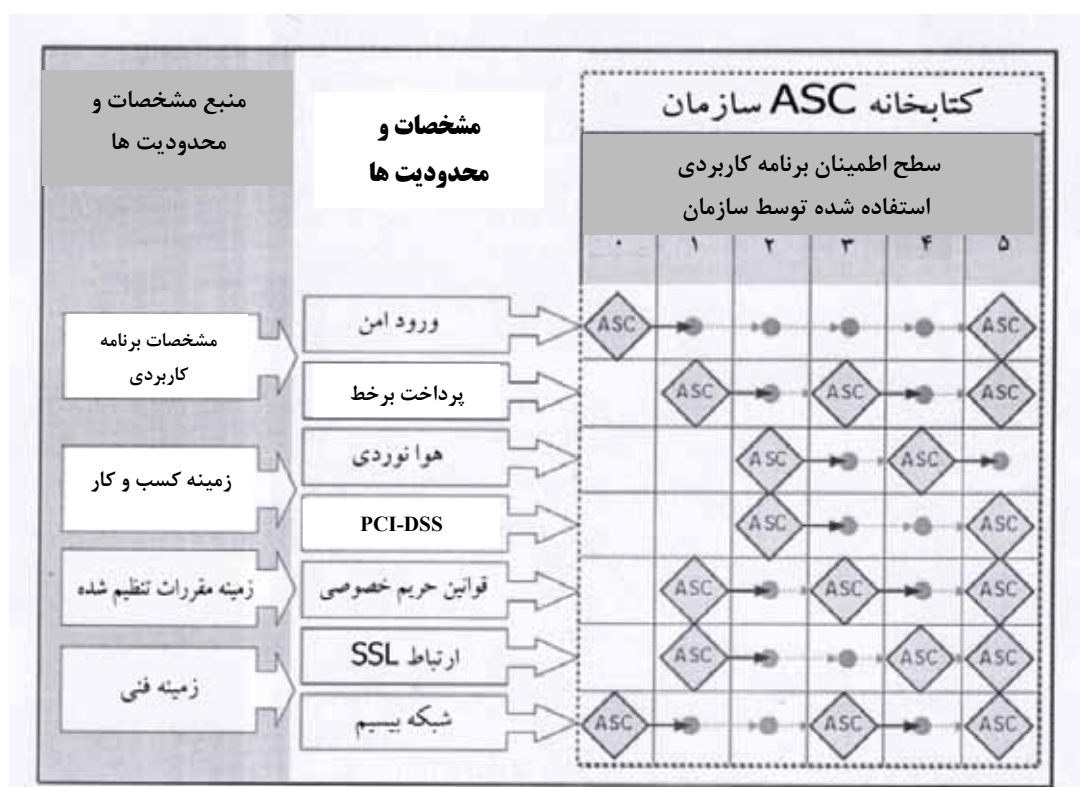
کنترل‌های امنیت برنامه کاربردی موجود در این کتابخانه در مجموعه‌هایی براساس سطح حفاظتی که در مقابل تهدیدهای امنیتی فراهم می‌کنند، چیده شده‌اند. هر مجموعه نشانه‌ای با عنوان «سطح اعتماد» می‌پذیرد تا مدیران را از درجه امنیت کسب‌شده از مجموعه کنترل‌های تعریف‌شده ی مشخص آگاه سازد. اگر برای مجموعه‌ای از کنترل‌ها سطح پایینی از اطمینان توصیف شده باشد، آن مجموعه حفاظت محدودی از

امنیت اطلاعات فراهم می‌کند. اگر برای مجموعه‌ای از کنترل‌ها سطح بالایی از اطمینان توصیف شده باشد، آن مجموعه سطح بالایی از حفاظت را فراهم می‌کند. سطوح اعتماد بیشتر در زیربند ۸-۱-۲-۶-۴ توصیف شده‌اند.

ASC‌های دقیق و مفصل هر پروژه برنامه کاربردی از میان کتابخانه ASC سازمانی انتخاب می‌شوند.

#### ۸-۱-۲-۶-۲ مثال کتابخانه ASC سازمان

شکل ۵ مثال ساده‌ای از کتابخانه ASC سازمانی موجود را نشان می‌دهد. سازمان این مثال برنامه‌های کاربردی را در زمینه هوانوردی توسعه می‌دهد. کتابخانه تمام کنترل‌های مورد نیاز سازمان برای پیاده‌سازی کارکردها، بهترین تجربه‌ها، استانداردها و قوانین و مقررات قابل کاربرد را شامل می‌شود.



شکل ۵- نمایش گرافیکی مثالی از کتابخانه ASC سازمان

در این مثال سازمان دو مشخصه برنامه کاربردی را تعریف کرده‌است: برقراری ارتباط امن و پرداخت اینترنتی. زمینه کسب و کاری که این سازمان خاص در آن قرار دارد، زمینه هوانوردی است و این زمینه استاندارد صنعتی PCI-DSS را پیاده‌سازی می‌کند. زمینه مقررات تنظیم‌شده رعایت برخی از قوانین حریم خصوصی را تحمیل می‌کند. زمینه فنی نشان می‌دهد که این سازمان کنترل‌های ارتباطات SSL و شبکه بی‌سیم را تعریف کرده‌است.



این مثال ساده نشان می‌دهد که مشخصات برنامه کاربردی سازمان و همچنین زمینه کسب و کار، مقررات تنظیم‌شده و فنی آن، محتویات کتابخانه ASC یک سازمان را مشخص می‌کند. به این ترتیب کتابخانه ASC هر سازمان مختص آن سازمان خاص خواهد بود.

#### ۸-۱-۲-۶-۳ فرآیند ایجاد کتابخانه ASC سازمان

فرآیند ایجاد کتابخانه ASC سازمان بسیار ساده است و حتی برای کوچک‌ترین سازمان‌ها به راحتی قابل اجرا است.

کتابخانه در ابتدا خالی است. ASC ها با گروه‌بندی در ستون‌هایی که مطابق سطح اعتماد آنها است ( به ستون‌های شکل ۵ مراجعه شود) اضافه می‌شوند. ممکن است سازمانی به بیش از یک سطح اعتماد برای برنامه‌های کاربردی نیاز داشته باشد.

مسئولیت کمیته ONF است که یک کتابخانه ASC بسازد تا نیازهای خاص و الزامات سازمان را تأمین کند. با تحلیل برنامه‌های کاربردی موجود یا جدید سازمان، به بهترین شکل به مقصود می‌رسیم. این تحلیل مشخص کردن مخاطره‌ها و الزامات امنیتی برای برنامه کاربردی است و سپس انتخاب یا ایجاد ASC های درخور آن الزامات را دربر می‌گیرد. برای هر برنامه کاربردی که تحلیل می‌شود نتیجه، مجموعه‌ای از ASC ها است.

این مجموعه از ASC ها می‌تواند از سه راه با کتابخانه ASC موجود تطابق داشته باشد.

الف) تمام مجموعه ASC ها از قبل شامل سطح اعتماد کتابخانه است که در این صورت هیچ چیز به کتابخانه اضافه نمی‌شود.

ب) یکی از سطوح اعتماد موجود با مجموعه کامل ASC ها تطابق نزدیکی دارد که در این صورت کتابخانه با ASC های مجموعه می‌تواند کامل شود.

پ) سطح اعتماد جدیدی از مجموعه ASC ها در کتابخانه ایجاد می‌شود.

بنابراین ممکن است سازمانی تصمیم بگیرد یا از تخصص‌های موجود و از طریق استفاده مجدد از کنترل‌های امنیتی برنامه‌های کاربردی موجود کنترل‌ها را بسازد یا کنترل‌های جدیدی تولید کرده یا به دست آورد، یا هر دوروش را به کار گیرد.

کتابخانه ASC سازمان در پاسخ به بازخورد هر پروژه برنامه کاربردی جدید همان‌طور که در زیربند ۸-۱-۳-۲ مطرح شده است، گسترش پیدا می‌کند.

#### ۸-۱-۲-۶-۴ سطح اعتماد برنامه کاربردی

سطح اعتماد برنامه کاربردی نشانه‌ای است که ارتباط میان کنش‌گرها از زمینه‌های مختلف را با اشکال مختلف دخالت آنها در امنیت برنامه کاربردی درون سازمان به‌طور ساده بیان می‌کند. سطح اعتماد برنامه کاربردی توسط سازمان و به‌منظور تشخیص واضح مجموعه‌ای خاص از کنترل‌ها تعریف می‌شود.

مثال ۱- در شکل ۵، سازمان ۶ سطح اعتماد تعریف کرده است که با ستون‌های سمت راست که از ۰ تا ۵ نشان‌گذاری شده‌اند نمایش داده شده است.

**مثال ۲-** در شکل ۵، سطح اعتماد «۱»، مجموعه‌ای از ASCها را مشخص می‌کند که مربوط به پرداخت اینترنتی، قوانین حریم خصوصی و ارتباطات SSL هستند. علاوه بر این، ASCهای مربوط به برقراری ارتباط امن و بی‌سیم که در سطح اعتماد صفر تعریف شده‌اند، همان‌طور که با فلش‌هایی که به نقطه‌ها ختم می‌شوند نشان داده شده‌اند، در سطح ۱ نیز به‌کار می‌روند.

سطح اعتماد برنامه کاربردی برخلاف مفهوم مخاطره که حاصل محاسبات تحلیل مخاطره است، حاصل محاسبه نیست. به این ترتیب، سطح اعتماد تکمیل‌کننده مخاطره نیست.

بلکه سطح اعتماد، مشابه مفهوم «نقشه امنیتی»، مجموعه‌ای از کنترل‌های تصویب‌شده سازمان به‌منظور کاهش مخاطره مشخص‌شده در تحلیل مخاطره، است. برای هر سازمان، هر سطح اعتماد مشابه نقشه امنیتی از پیش تعریف‌شده و قابل استفاده مجدد است.

سازمان باید حدود (یا زمینه یا مقیاس) سطح اعتماد خود را تعریف کند تا کمیته ONF سازمان آنها را به‌عنوان ارزش‌های ممکن سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی تصویب کند. این حدود به هر شیوه‌ای که مناسب سازمان است می‌تواند تعریف شوند.

**مثال ۳-** یک سازمان ممکن است همان‌گونه که در شکل ۵ نشان داده‌شده از سطوح عددی ۰ تا ۵ استفاده کند. سازمان دیگری ممکن است زمینه‌ای از ارزش‌های تعریف‌شده مانند (کم و متوسط و بالا) یا (سبز، زرد، قرمز) را به‌کارگیرد. سازمان دیگری ممکن است از معیارهایی برپایه معیار پذیرش مخاطره استفاده کند.

توصیه می‌شود سازمان سطح اعتماد قابل پذیرش حداقلی را برای هر یک از برنامه‌های کاربردی خود تعریف کند. در این استاندارد ملی برای تعریف سطح اعتماد قابل پذیرش حداقل (در مقابل سطح اعتماد قابل پذیرش حداکثر) از نام «سطح اعتماد صفر» استفاده می‌کند. یک سازمان ممکن است از هر نامی برای این سطح اعتماد استفاده کند.

توصیه می‌شود سازمان بر سطح اعتماد دست‌یافته توسط برنامه‌های کاربردی نظارت کند و اگر در هر زمان برنامه کاربردی پایین‌تر از سطح ۰ قرارگرفت، به‌ویژه بعد از استفاده مفید از آن، دست به اقدام اصلاحی بزند.

**مثال ۴-** در شکل ۵ کمیته ONF در سطح اعتماد صفر برای تمام برنامه‌های کاربردی که از ارتباط امن یا ارسال بی‌سیم استفاده می‌کنند، یک ASC تعریف کرده است. حتی اگر سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی مشخص با تحلیل مخاطره این برنامه کاربردی، سطح اعتماد صفر باشد، این ASC همچنان باید اجرا شود.

## ۸-۱-۲-۶-۵ کنترل امنیت برنامه کاربردی

### ۸-۱-۲-۶-۵-۱ کلیات

کنترل امنیت برنامه کاربردی در استاندارد ISO/IEC 27034 مفهومی محوری است. این مفهوم برای معرفی فعالیت‌های امنیتی در چرخه حیات برنامه کاربردی استفاده می‌شود و شواهد اثباتی مورد نیاز برای تأیید برنامه کاربردی موفق را بیان می‌کند.

مفهوم کنترل امنیت برنامه کاربردی به‌طور گسترده در صنعت امنیت اطلاعات استفاده می‌شود. از منابعی مانند استاندارد ISO/IEC 15408-3 و NIST انتشار ویژه 800-53 هزاران کنترل امنیت مرتبط منتشر می‌شوند و به شکل گسترده در دسترس هستند.

ASC، کنترل امنیتی است که در پروژه‌های برنامه‌های کاربردی استفاده می‌شود و با استفاده از ساختاری دقیق که در بندهای زیرمجموعه زیر آمده است تعریف می‌شود. پیوست ب مثالی ارائه می‌دهد که چگونگی توصیف کنترل‌های امنیت NIS SP 800-53 را با استفاده از ساختار ASC توضیح می‌دهد.

برای سازمان‌هایی که مفهوم ضمانت را همان‌گونه که در استاندارد ISO/IEC TR 15026-2 تعریف شده، پیاده‌سازی کرده‌اند، ASCها برای مدیریت آسان و فراهم آوردن به‌موقع شواهد مورد نیاز برای پشتیبانی ادعاها و استدلال‌های مربوط به امنیت یک برنامه کاربردی مفید هستند. پشتیبانی بیشتر از استدلال‌ها با به‌کارگیری مداوم فرآیندهای پیشنهادی این IS برای ایجاد، تأیید و استفاده از هر ASC تأمین می‌شود. از آنجایی که کل مجموعه ASCهای انتخاب‌شده برای پروژه برنامه کاربردی از تحلیل مخاطره امنیت برنامه کاربردی سرچشمه می‌گیرند، این مجموعه ادعاها سطح بالایی، توجیهات و استدلال‌های مربوط به امنیت برنامه کاربردی را به‌طور مستقیم پشتیبانی می‌کند.

ASCها می‌توانند در موارد زیر مورد استفاده قرار گیرند:

الف) امن کردن مولفه‌های برنامه کاربردی از جمله نرم‌افزار، داده، نرم‌افزارهای تجاری و عمومی و زیر-ساخت

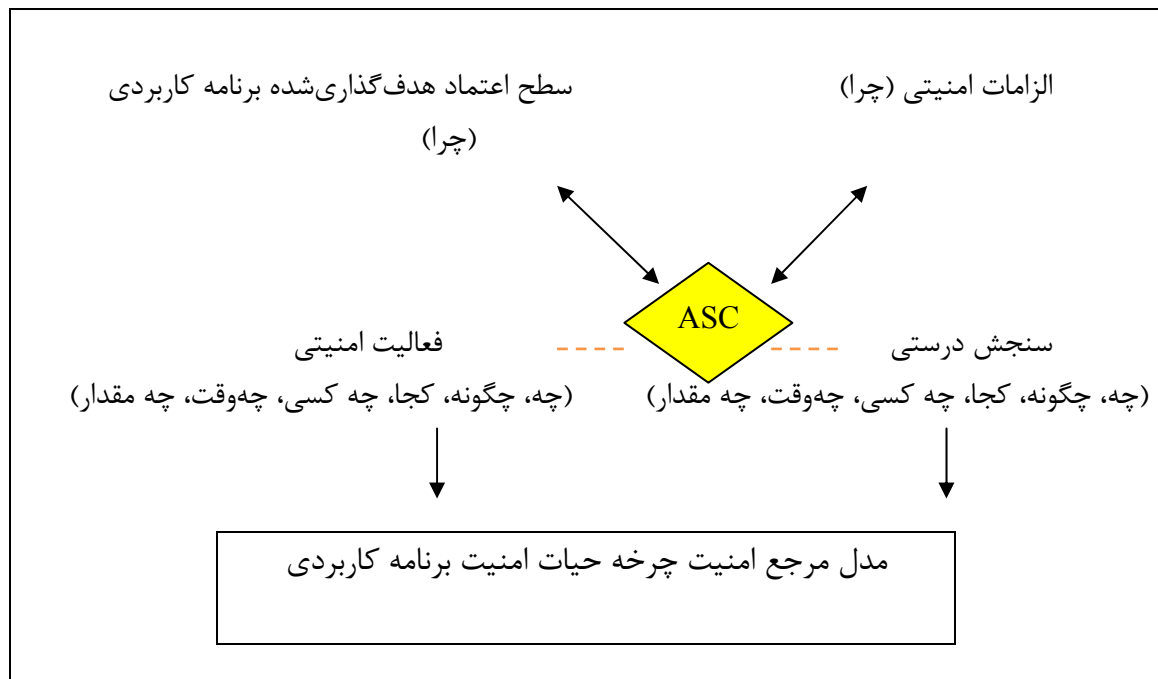
ب) افزودن فعالیت‌های امنیتی به فرآیندهایی که در مراحل چرخه حیات برنامه کاربردی استفاده می‌شوند.

پ) تأیید جایگاه‌ها، مسئولیت‌پذیری‌ها و صلاحیت‌های حرفه‌ای کلیه کنش‌گرهای درگیر در یک پروژه

ت) تعیین معیار ارزیابی/پذیرش اجزا

ث) کمک در تعیین سطح اعتماد واقعی برنامه کاربردی

شکل ۶ نشان می‌دهد که ASC برای گروه پروژه برنامه کاربردی (برای مثال جهت کاهش یا محدود کردن یک مخاطره امنیتی خاص) فعالیت امنیتی فراهم می‌کند و برای گروه تأیید فعالیت سنجش درستی را (برای مثال برای تأیید این‌که فعالیت امنیتی مربوطه با بررسی شواهد موافق با موفقیت اجرا شده است) فراهم می‌آورد.

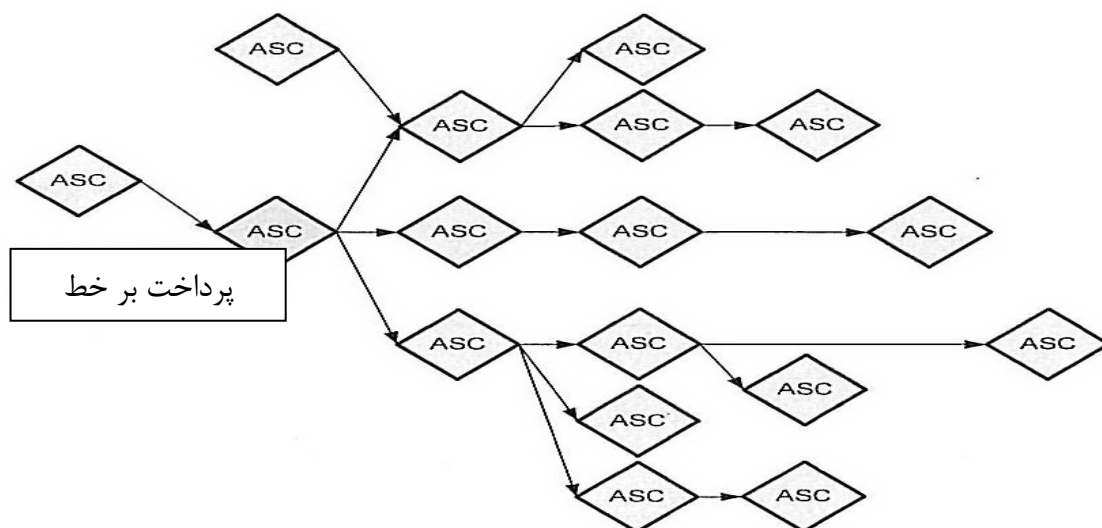


شکل ۶- اجزای یک ASC

قسمت فعالیت ASC چگونگی برخورد با مسائل امنیتی یک پروژه برنامه کاربردی را مشخص می کند. قسمت سنجش ASC چگونگی تأمین شواهد دال بر این که فعالیت به درستی، توسط کنش گری با صلاحیت انجام شده است و نتایج مورد انتظار فراهم شده است را مشخص می کند. فعالیت و سنجش، هر دو هزینه تخمینی را فراهم می کنند که به سازمان در ارزیابی و تأیید هزینه های کلی کنترل های امنیت مربوط به سطح اعتماد هدف گذاری شده، کمک می کند. ASC ها می توانند در یک نمودار به هم متصل شوند به این ترتیب می توان فعالیت را پس از اجرا شدن در ASC توسط فعالیت های خرد ادامه داد. این ویژگی ASC در موارد زیر مفید است:

- الف) تأمین تنها اطلاعات مرتبط با کنش گره های مختلف از طریق پنهان کردن پیچیدگی های غیرضروری
- ب) تسهیل ارتباطات از طریق گروه بندی ASC های مرتبط تحت یک عنوان و با استفاده از واژگان مناسب. برای مثال، استفاده از زبان سطح کسب و کار هنگام برقراری ارتباط با مدیران
- پ) تسهیل توزیع ASC ها از طریق گروه بندی آنها در مجموعه های مرتبط
- ت) تضمین اینکه تمام فعالیت های امنیتی در ASC های متصل اجرا شده و هیچکدام کنار گذاشته نشده اند.

شکل ۷ مثالی از این رابطه نموداری را نشان می دهد که در آن مجموعه ای از ASC ها تحت عنوان «پرداخت اینترنتی» به هم متصل شده اند. در این مثال، تمام ASC های مربوط به پرداخت اینترنتی می توانند به عنوان مجموعه ای واحد استفاده شوند و در صورت لزوم این پیچیدگی پنهان شود.



شکل ۷- نمودار ASC ها.

ASC ساختار داده‌ای پیچیده‌ای است که جزئیات بیشتر آن در قسمت ۵ استاندارد حاضر تحت عنوان: «پروتکل‌ها و ساختار داده ASC» مطرح خواهد شد. مرور کلی مختصری در زیر آمده است.

**یادآوری -** هر چند استاندارد ISO/IEC 27034-5 ساختار ASC را رسمی خواهد کرد، اما ممکن است سازمان‌ها هنوز برای راهنمایی در مورد مشخص کردن موارد اطلاعاتی که قرار است در طول چرخه حیات برنامه‌های کاربردی تولید شوند به استاندارد ISO/IEC 15289 مراجعه کنند.

#### ۸-۱-۲-۶-۵-۲ شناسایی ASC

قسمت شناسایی ASC شامل اطلاعاتی از قبیل موارد زیر است:

- (الف) اطلاعات ASC: نام، شناسه، مؤلف، تاریخ و توصیف ASC
- (ب) نشانگرهایی به ASC های والد و ASC های فرزند (یک ASC تواند به صورت ساختار نموداری ارائه شود).
- (پ) نشانگرهایی به زمینه‌های کسب و کار، مقررات تنظیم‌شده و فنی مرتبط و همچنین مشخصاتی از برنامه کاربردی که الزامات امنیتی این ASC را فراهم می‌کنند.

#### ۸-۱-۲-۶-۵-۳ هدف ASC

هدف ASC، دلیل وجود ASC یعنی الزامات امنیتی که این ASC برای آنها طراحی شده است را مشخص می‌کند.

هدف ASC موارد زیر را مشخص می‌کند:

- (الف) کدام یک از عناصر فعالیت امنیتی باید شواهد اثباتی مرتبط با سنجش تأیید را فراهم کند.
- (ب) ASC برای کدام سطح اعتماد، اجباری است.

پ) مشخصات یا الزامات برنامه کاربردی که این ASC به آنها مربوط می‌شود و می‌توانند به مقررات تنظیم‌شده، استانداردها و بهترین روش‌های کاربردی اشاره کنند.

ت) تهدیدهای امنیتی و فرضیاتی در مورد محیط بهره‌برداری برنامه کاربردی یک ASC می‌تواند به چندین سطح اعتماد مرتبط شود.

**مثال در شکل ۵ -** در سطح ۱ هر برنامه کاربردی درگیر در پرداخت اینترنتی، یک ASC تعریف شده است. این ASC برای تمام پروژه‌هایی ضروری است که برنامه کاربردی درگیر در پرداخت اینترنتی را توسعه می‌دهند و سطح اعتماد هدف‌گذاری شده توسط مالک برنامه کاربردی از ۱ تا ۲ مقرر شده است. اگر مالک برنامه خواهان مقرر کردن سطح اعتماد هدف‌گذاری شده ۳ برای برنامه کاربردی باشد، یک ASC با فعالیت امنیتی قوی‌تر و/یا سنجش امنیت قوی‌تر مورد نیاز است.

#### ۸-۱-۲-۳-۴ فعالیت امنیتی ASC

این عنصر گام‌ها یا رویه‌های لازم برای پیاده‌سازی فعالیت را توصیف می‌کند و حداقل باید موارد زیر را تعریف کند:

الف) چیست:

۱) توصیف کامل فعالیت امنیتی

۲) پیچیدگی فعالیت

۳) محصولات مصنوعی تولیدشده توسط فعالیت. این محصول مصنوعی شواهد اثباتی لازم برای نشان‌دادن حضور برنامه کاربردی معرفی‌شده، فرآیندها یا رویه‌های کنترل امنیت (برای مثال فعالیت ASC) را بیان می‌کند.

۴) نتایج مورد انتظار فعالیت ASC (یعنی توصیفی از شرایط، وضعیت یا ارزش دقیق محصول مصنوعی تولیدشده توسط این فعالیت)

ب) چگونه :

فنون اجرای این فعالیت و به‌دست‌آوردن محصول مصنوعی، مانند شناسایی کد منبع استفاده شده برای پیاده‌سازی ارتباطات امن با یک خدمت LDAP، شناسایی کتابخانه مورد استفاده قرارگرفته برای رمزبندی یا سندی که برای انجام فعالیت، راهنمایی فراهم می‌کند.

ج) کجا:

هدف فعالیت امنیتی، مانند کد منبع، پارامترهای برنامه کاربردی، اجزای زیرساختی، فرآیند

د) چه کسی:

صلاحیت‌های مورد نیاز برای کنش‌گرهایی که باید این فعالیت را اجرا کنند. ASCها به کنش‌گرها محول می‌شوند، (احتمالاً در شکل انتساب‌های رسمی سازمانی) زیرا سازمان باید اطمینان حاصل کند که صلاحیت‌های حرفه‌ای هر جایگاه کسب شده‌اند و اصل تفکیک وظایف مورد ملاحظه قرار گرفته‌است. ASCها باید برای مقصود صریح تأیید صلاحیت‌های حرفه‌ای نگاشته شوند.

ه) چه وقت:

اشاره به یک فعالیت خاص در مرحله‌ای از مدل مرجع چرخه حیات امنیت برنامه کاربردی (زیربند ۸-۱-۲-۷ مراجعه شود). که این فعالیت باید در آن اجرا شود.

(و) چقدر:

هزینه تخمینی انجام این فعالیت ASC.

#### ۸-۱-۲-۶-۵-۵-سنجش تأیید ASC

این بخش کنترل تأییدی را ارائه می‌دهد که برای تأیید موفقیت اجرای فعالیت ASC مرتبط اجرا می‌شود. سنجش تأیید حداقل باید موارد زیر را تعریف کند:

(الف) چیست:

(۱) توصیف کامل سنجش امنیت. این توصیف چگونگی درستی سنجی وجود و صحت محصول مصنوعی تولیدشده توسط فعالیت ASC نشان می‌دهد.

(۲) پیچیدگی سنجش

(۳) محصول مصنوعی تولیدشده توسط این سنجش. این محصول مصنوعی شواهد اثباتی لازم را بیان می‌کند تا نشان دهد ASC درستی سنجی شده است.

(۴) نتایج مورد انتظار (موقعیت، وضعیت یا توصیف دقیق ارزش محصول مصنوعی)

(ب) چگونه:

فنون اجرای این سنجش و به‌دست‌آوردن محصول مصنوعی مانند ابزارها و زمینه بازبینی کد یا سندی که راهنمایی اجرای سنجش را فراهم کند.

(ج) کجا:

هدف فعالیت درستی سنجی، یعنی خصوصیات دقیق محصول مصنوعی تولیدشده توسط فعالیت ASC مرتبط که مورد درستی سنجی قرار می‌گیرد.

(د) چه کسی:

صلاحیت‌های حرفه‌ای مورد نیاز کنش‌گرهای درگیر در کنترل تأیید. ASCها به کنش‌گرها محول می‌شوند، (احتمالاً در شکل انتساب‌های رسمی سازمانی) زیرا سازمان باید اطمینان حاصل کند که صلاحیت‌های حرفه‌ای هر جایگاه کسب شده‌اند و اصل تفکیک وظایف مورد ملاحظه قرار گرفته است. ASCها باید برای مقصود صریح تأیید صلاحیت‌های حرفه‌ای نگاشته شوند.

(ه) چه وقت:

اشاره به یک فعالیت خاص در مرحله‌ای از مدل مرجع چرخه حیات امنیت برنامه کاربردی (زیربند ۸-۱-۲-۷ مراجعه شود). که این سنجش در آن باید انجام گیرد. در صورت نیاز، این سنجش می‌تواند به‌صورت دوره‌ای برگزار شود.

(و) چقدر:

هزینه تخمینی یک بار رخداد این فعالیت سنجش درستی.

## ۸-۱-۲-۷ مدل مرجع چرخه حیات برنامه کاربردی

### ۸-۱-۲-۷-۱ کلیات

سازمانی که درگیر تولید، برون‌سپاری یا اکتساب برنامه کاربردی است معمولاً چارچوبی از فرآیندهای تعریف-شده و فعالیت‌های طبقه‌بندی‌شده را به‌صورت مرحله‌ای استفاده می‌کند. این چارچوب «مدل چرخه حیات» نامیده می‌شود. با توجه به زمینه مورد استفاده، این عبارت به «مدل چرخه حیات برنامه» یا «مدل چرخه حیات سامانه» یا «مدل چرخه حیات نرم‌افزار» اشاره دارد. این مطلب مفهوم تازه‌ای نیست که توسط این استاندارد ملی ارائه شده باشد، بلکه تعریف آن را می‌توان در استانداردهای ISO/IEC 12207 و ISO/IEC 5288 مشاهده نمود.

این‌گونه چارچوب‌ها مختص هر سازمان است. این چارچوب در طی سال‌ها استفاده و پالایش شده است. چرخه حیات یک برنامه کاربردی خاص برای مثال تکامل برنامه کاربردی از آغاز شکل‌گیری تا زمان کنارگذاشته‌شدن نمونه‌ای از مدل چرخه حیات سازمان است.

ممکن است گروه‌های مختلف در سازمان‌های پیچیده، برای پروژه‌های مختلف از مدل‌های چرخه حیات برنامه کاربردی متفاوتی استفاده کنند. این امر معمولاً در سازمان‌های بزرگی اتفاق می‌افتد که از طریق ادغام یا تمرکززدایی ایجاد شده‌اند. سازمان‌های دیگر مدل‌های چرخه حیات برنامه کاربردی تخصصی متفاوتی ایجاد کرده‌اند که به زمینه‌های برنامه کاربردی خاص مانند برنامه‌های کاربردی شبکه، برنامه‌های کاربردی زمان واقعی، برنامه‌های کاربردی جاسازی‌شده، برنامه‌های کاربردی پزشکی و غیره مربوط می‌شوند.

فعالیت‌های انجام شده در طی مراحل چرخه حیات برنامه کاربردی یک نرم‌افزار یا یک سامانه، قسمتی از فرآیندهای سطح سازمانی هستند که باید با نیازهای الزامی ارائه شده در استاندارد ISO/IEC 12207 و استاندارد ISO/IEC 5288 سازگار باشند. به‌علاوه، استاندارد ISO/IEC TR 24748 راهنمایی بیشتری نیز ارائه کرده و مدل‌هایی برای چرخه حیات توسعه سامانه و نرم‌افزار، مراحل چرخه حیات و ارتباطات آنها با فرآیندهای چرخه حیات توصیف کرده است.

این استاندارد ملی تغییری در مدل چرخه حیات برنامه کاربردی سازمان تحمیل نکرده یا حتی پیشنهاد هم نمی‌کند، بلکه فعالیت‌هایی با عنوان کنترل امنیت برنامه کاربردی (ASC) به فعالیت‌های معمول در مراحل تعریف شده در مدل چرخه حیات برنامه کاربردی سازمان اضافه می‌کند.

همان‌گونه که قبلاً در زیربند ۸-۱-۲-۶-۵ مطرح شد، ASCها شامل نشانگرهایی هستند که به نقطه خاصی در چرخه حیات اشاره دارند و مشخص می‌کنند چه زمانی فعالیت‌های امنیتی و سنجش تأیید باید انجام شوند.

در حال حاضر مدل‌های مختلفی از مدل چرخه حیات برنامه کاربردی و سامانه وجود دارد که یک سازمان می‌تواند برای نیازهای داخلی خود از بین آنها انتخاب کند. برای این استاندارد ملی نه مقدور و نه مطلوب است که به همه آنها مراجعه کرده یا یکی را بر دیگری ترجیح دهد. بنابراین غیر ممکن است که یک ASC در استاندارد موجود باشد که مستقیماً به یک مرحله فرآیند یا فعالیت در یک مدل چرخه حیات خاص اشاره داشته باشد. این مسئله امکان انتقال مفهوم ASC این استاندارد ملی را به سازمان‌های موجود در جوامع



گسترده‌تر کاهش می‌دهد. راه حل این مشکل، ارائه یک مدل مرجع چرخه حیات امنیت برنامه کاربردی به‌عنوان یک مرجع استاندارد جهت اضافه کردن ASCها به فعالیتهای اجرا شده درباره مدیریت برنامه کاربردی، تهیه و به‌کارگیری برنامه کاربردی، مدیریت زیرساخت و ممیزی برنامه کاربردی است. این مدل نمایشی از مراحل و فعالیتهای معمول در مدل‌های چرخه حیات برنامه کاربردی است.

این مدل محدود به توسعه نرم‌افزار نیست، بلکه مرجعی است برای فعالیتهای زمینه‌های دیگر مانند سرپرستی، نگهداری نرم‌افزار و زیرساخت، مدیریت پروژه، ممیزی و کنترل هدف مدل چرخه حیات امنیت برنامه کاربردی این است که:

الف) به سازمان کمک کند تا به هر یک از چرخه‌های حیات برنامه کاربردی خود، با مشخص کردن تمام فرآیندها و کنشگرهای بالقوه مرتبط با امنیت برنامه کاربردی اعتبار بخشد.

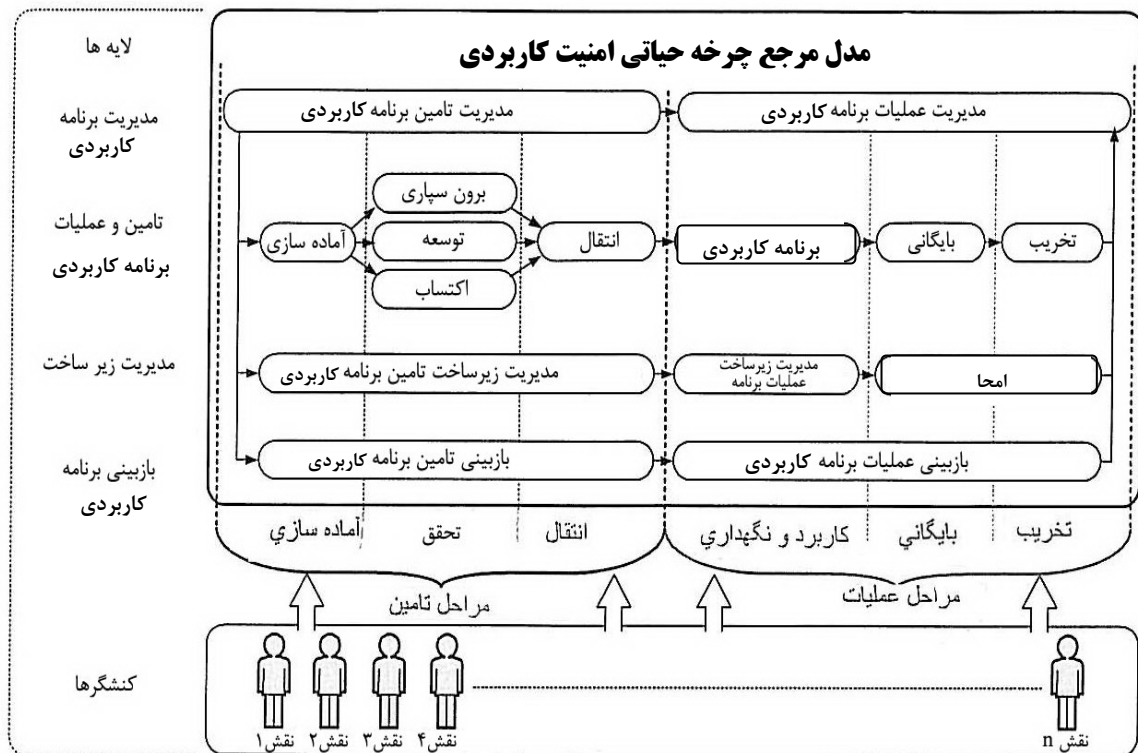
ب) به سازمان کمک کنند که توجه صحیح به تمام نگرانی‌های امنیتی در تمامی مراحل چرخه‌های حیاتی برنامه را تضمین کند.

پ) به سازمان‌ها کمک کند تا هزینه و شدت اثر اعمال تجربه‌های این استاندارد ملی را در پروژه‌های برنامه کاربردی خود از طریق حفظ چرخه‌های حیات برنامه کاربردی موجود به حداقل برسانند.

ت) با وجود چرخه‌های حیات متفاوت برنامه کاربردی برای سازمان، مدلی استاندارد برای جهت به‌اشتراک‌گذاری ASCها بین تیم‌های پروژه فراهم می‌کند.

ث) با وجود چرخه‌های حیات متفاوت برنامه کاربردی، برای سازمان مدلی استاندارد برای جهت به‌اشتراک‌گذاری ASCها با سازمان‌های دیگر فراهم می‌کند.

شکل ۸ نمایش نموداری مدل مرجع چرخه حیات امنیت برنامه کاربردی ارائه شده در این استاندارد ملی است.



شکل ۸- نمای سطح بالا از مدل مرجع چرخه حیات امنیت برنامه کاربردی

سازمان باید ارتباطی پایدار بین مراحل و فعالیت‌های تعریف شده در این مدل مرجع و مراحل و فعالیت‌های مورد استفاده در مدل‌های خود برقرار کند. این امر راه‌کاری برای نشان دادن نقاطی که ASCها به مراحل و فعالیت‌های سازمان اعمال می‌شوند ارائه می‌کند.

کمیته ONF سازمان پیاده‌سازی ASCها را در مدل مرجع چرخه حیات امنیت برنامه کاربردی تعیین می‌کند. این اقدام تخصیص پیگیری یکنواخت ASCها با حداقل قابل قبول جهت سطح اعتماد هدف‌گذاری شده را در طول راه‌اندازی برنامه‌ریزی تمام پروژه‌های برنامه کاربردی سازمان تضمین می‌کند. مدل مرجع به‌طور افقی به دو قسمت تقسیم شده است: تأمین که در آن فعالیت‌ها جهت به‌دست آوردن و اجرای برنامه انجام می‌شوند و عملیات که فعالیت‌های پس از توزیع آن انجام می‌شوند.

تأمین و عملیات می‌توانند به مراحل زیر تقسیم شوند:

(الف) مراحل تأمین شامل سه مرحله: آماده‌سازی، تحقق و انتقال،

(ب) مراحل عملیات شامل سه مرحله: کاربرد و نگهداری، بایگانی، امحا.

مدل مرجع به‌صورت عمودی به چهار لایه اصلی تقسیم می‌شود:

(الف) مدیریت برنامه: این لایه از فعالیت‌های در زمینه سرپرستی، مانند مدیریت پروژه و مدیریت عملیات برنامه تشکیل شده است. این فعالیت‌ها در حیطه فرآیندهای تعریف شده در ISMS سازمان انجام می‌پذیرند.

(ب) تهیه و به‌کارگیری برنامه کاربردی: این لایه از فعالیت‌های مربوط به تهیه و استفاده از خود برنامه کاربردی تشکیل شده است. این فعالیت‌ها معمولاً در حیطه فرآیندهای پیشنهادی استانداردهایی مانند سری

استاندارد ISO/IEC 15026، استاندارد ISO/IEC 5288، استاندارد ISO/IEC 12207 و استاندارد ISO/IEC 21827 انجام می‌پذیرند.

ج) مدیریت زیر ساخت: این لایه از فعالیت‌های مربوط به مدیریت خدمات IT در سازمان تشکیل شده است که از برنامه پشتیبانی می‌کنند. این فعالیت‌ها معمولاً در حیطه فرآیندهای پیشنهادی استانداردهایی مانند استاندارد TR 20000-4 و محصولات راهنما مانند ITIL انجام می‌پذیرند.

د) بازبینی برنامه: این لایه متشکل از فعالیت‌های مربوط به کنترل و صحت‌سنجی است. اینگونه فعالیت‌ها معمولاً در فرایندهای پیشنهادی استانداردهایی مانند استاندارد ISO/IEC 5288، استاندارد ISO/IEC 12207 و اسناد تجارب صنعتی مانند CobiT اجرا می‌شوند.

کنشگرها شامل تمام افراد درگیر در تمام سطوح و لایه‌های مدل مانند مدیران پروژه، تدوین‌گران مدیران سامانه بانک اطلاعاتی، مدیران کاربری، صاحبان برنامه، ممیزین مصرف‌کننده‌های نهایی، تکنسین‌های پشتیبانی، مدیران شبکه و غیره است.

فعالیت‌های معمول در مراحل مدل مرجع چرخه حیات امنیتی برنامه که در شکل ۸ نیز نشان داده شده به‌طور زیر توصیف می‌شوند.

#### **۸-۱-۲-۷-۲ مدیریت تأمین برنامه کاربردی**

فعالیت‌های مربوط به مدیریت تأمین برنامه کاربردی توسط مدیران پروژه و مدیران اداری در طی مراحل تأمین از چرخه حیاتی برنامه اجرا می‌شوند.

اینگونه فعالیت‌ها به‌عنوان قسمتی از فرایندها در سطح سازمان اجرا می‌شوند و شامل فرایندهای مهندسی نرم‌افزار از گروه فرایندهای پروژه تعریف‌شده در استاندارد ISO/IEC 12207 از قبیل فرایند مدیریت منابع انسانی، فرایند برنامه‌ریزی پروژه، فرایند ارزیابی و کنترل پروژه و فرایند مدیریت تصمیم‌گیری است.

#### **۸-۱-۲-۷-۳ مدیریت عملکرد برنامه کاربردی**

فعالیت مدیریت عملکرد برنامه کاربردی به مدیریت و استفاده از برنامه کاربردی در طی مراحل عملیات مربوط می‌شود.

این فعالیت‌ها معمولاً به‌عنوان قسمتی از فعالیت‌ها در سطح سازمانی انجام می‌شود و شامل فرایندهای مهندسی نرم‌افزار در استاندارد ISO/IEC 12207 مانند فرایند مدیریت تصمیم‌گیری و فرایند مدیریت اطلاعات است.

معمولاً مسئولیت برنامه به عهده مالک بوده و مالک است که تصمیم می‌گیرد قسمتی از مسئولیت خود را به کنشگرهای دیگری مانند مدیران کاربران واگذار کند.

تغییرات برنامه کاربردی در مراحل عملیات مانند تغییراتی که ناشی از مقررات جدید در مورد تهدیدها یا نیازمندی‌ها است، باید توسط صاحب برنامه که مسئول ضمانت صحت و تداوم عملکرد برنامه در رابطه با نیازهای امنیتی متغیر سازمان است اعمال شوند.

از طریق این فرایندها صاحب برنامه شواهد و تضمین مورد نیاز جهت اعتماد از توجه به اداره پروژه اجرایی را به ISMS سازمان ارائه می‌کند.

#### ۸-۱-۲-۷-۴ آماده‌سازی

در طی مرحله آماده‌سازی، تیم تأمین برنامه کاربردی فعالیت‌های اولیه یا آماده‌سازی را انجام می‌دهد. این فعالیت‌ها معمولاً قسمتی از فرایند در سطح سازمانی هستند. از جمله فرایندهای مهندسی نرم‌افزار استاندارد ISO/IEC 12207 مانند زیربند ۶-۳-۳، فرایند مدیریت تصمیم‌گیری و زیربند ۶-۳-۶، فرایند مدیریت اطلاعات.

#### ۸-۱-۲-۷-۵ فرایندهای آماده‌سازی

این گروه از فرایندها شامل فعالیت‌های اجرا شده در حین مرحله آماده‌سازی یک پروژه اجرایی است.

**یادآوری-** این فرایند شامل فرایندهای مهندسی نرم‌افزار بخش ۶-۴-۱ استاندارد ISO/IEC 12207 فرایند تأمین نیازهای سهام‌داران، تحلیل نیازمندی‌های سامانه و مدیریت مخاطره است.

#### ۸-۱-۲-۷-۶ برون‌سپاری

در طی مرحله تحقق، فعالیت‌های مربوط به پیاده‌سازی نرم‌افزار توسط تیم تأمین به اجرا در می‌آیند. اگر سازمانی برخی فعالیت‌های پیاده‌سازی را به بیرون از سازمان می‌سپارد ممکن است نیاز پیدا کند ASC‌های ویژه‌ای به فعالیت‌های پیاده‌سازی خود اضافه کند تا سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی تحصیل شود. به همین دلیل مدل مرجع چرخه حیات امنیت برنامه کاربردی محدوده فعالیت ویژه‌ای برای برون-سپاری در نظر گرفته است.

اینگونه فعالیت‌ها معمولاً در سطح سازمان انجام می‌شوند و شامل فرایندهای مهندسی نرم‌افزار استاندارد ISO/IEC 12207 مانند فرایند اکتساب ثبت نرم‌افزار، فرایند مدیریت، فرایند مدیریت پیکربندی و برنامه و فرایند مدیریت مخاطرات هستند.

#### ۸-۱-۲-۷-۷ توسعه

فعالیت‌های مربوط به پیاده‌سازی نرم‌افزار توسط تیم تأمین در طی مرحله تحقق انجام می‌گیرد. چنانچه سازمان در حال اجرای برخی فعالیت‌های پیاده‌سازی به صورت داخلی باشد، ممکن است ASC‌های اضافه‌شده به این فعالیت‌های پیاده‌سازی با ASC‌های اضافه‌شده هنگام خرید یا برون‌سپاری پیاده‌سازی یا اجزای برنامه کاربردی متفاوت باشند. به همین دلیل مدل مرجع چرخه حیات امنیت برنامه کاربردی، محدوده ویژه‌ای برای فعالیت‌های توسعه‌ای که به پیاده‌سازی نرم‌افزارهای توسعه‌یافته داخلی منجر می‌شوند، ارائه می‌دهد. این فعالیت‌ها معمولاً قسمتی از فرایندهای در سطح سازمان هستند و در برگیرنده فرایندهای مهندسی نرم‌افزار در استاندارد ISO/IEC 12207 از جمله فرایند مدیریت مخاطره، طراحی معماری سامانه، فرایند طراحی معماری سامانه، جزئیات فرایند طراحی نرم‌افزار، فرایند ساخت نرم‌افزار، فرایند مدیریت اسناد نرم-افزاری، فرایند مدیریت پیکربندی نرم‌افزار، فرایند صحت‌سنجی نرم‌افزار، فرایند تأیید اعتبار نرم‌افزار، فرایند بازبینی نرم‌افزار، فرایند مهندسی زمینه و فرایند مدیریت استفاده مجدد از دارایی‌ها است.

#### ۸-۱-۲-۷-۸ اکتساب

فعالیت‌های اکتسابی به‌وسیله تیم تأمین و به‌منظور به‌دست آوردن یا خرید محصول یا خدمات مورد نیاز سازمان انجام می‌پذیرد. ASCهای خاصی ممکن است به این فعالیت‌ها اضافه شوند. به همین دلیل مدل ارجاعی چرخه حیاتی امنیت برنامه محل خاصی برای فعالیت‌های اکتسابی که منجر به پیاده‌سازی و اجرای برنامه به‌دست آمده می‌شوند، ارائه می‌کنند.

این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای در سطح سازمان هستند و دربرگیرنده فرایندهای مهندسی نرم‌افزار از استاندارد ISO/IEC 12207 از جمله فرایند اکتساب، فرایند مدیریت اسناد نرم‌افزاری، فرایند مدیریت پیکربندی نرم‌افزار، فرایند مدیریت مخاطره و فرایند پیاده‌سازی است.

#### ۸-۱-۲-۷-۹ انتقال

این قسمت از مرحله انتقال شامل فعالیت‌هایی است که توسط تیم تأمین جهت آماده‌سازی، پیکربندی آزمایش و توسعه برنامه کاربردی در محیط عملیاتی تعریف‌شده توسط سازمان انجام می‌شود. این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای در سطح سازمان هستند که دربرگیرنده فرایندهای مهندسی نرم‌افزار از استاندارد ISO/IEC 12207 از جمله فرایند مدیریت پیکربندی نرم‌افزار، فرایند یکپارچه‌سازی سامانه و فرایند آزمایش صلاحیت سامانه است.

#### ۸-۱-۲-۷-۱۰ به‌کارگیری

در طی مرحله به‌کارگیری و نگهداری، فعالیت‌هایی در رابطه با استفاده واقعی از برنامه در محیط عملیاتی توسط تمام کاربران، از جمله کاربران نهایی انجام می‌پذیرد. این فعالیت‌ها شامل مدیریت کاربر و دسترسی، برقراری ارتباط، نظارت، آموزش امنیت و غیره هستند. سایر فعالیت‌ها به هدف مدیریت نگهداری و تغییر نرم‌افزار انجام می‌شوند و دربرگیرنده به‌روزرسانی نرم‌افزار اجرایی به‌منظور برآورده کردن نیازهای اطلاعاتی متغیر مانند اضافه کردن کارکردهای جدید و تغییر قالب داده هستند. این فعالیت شامل اصلاح ایرادات و تطابق نرم‌افزار با سخت‌افزار جدید نیز هست. این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای در سطح سازمان هستند و دربرگیرنده فرایندهای مهندسی نرم‌افزار از استاندارد ISO/IEC 12207 مانند فرایند عملیات نرم‌افزاری و فرایند نگهداری نرم‌افزار است.

#### ۸-۱-۲-۷-۱۱ بایگانی

فعالیت‌های بایگانی توسط تیم عملیات در هنگامی که برنامه دیگر در حالت عملیاتی مورد نیاز نیست، انجام می‌شوند. این فعالیت‌ها شامل بایگانی تمام اطلاعات نرم‌افزار از جمله بایگانی تمام ابزارها و فرایندها به‌منظور حفاظت و دسترسی امن به اطلاعات هستند، حتی در زمانی که برنامه در محیط عملیاتی در حال اجرا نیست.

این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای در سطح سازمان بوده و دربرگیرنده فرایندهای مهندسی نرم‌افزار از استاندارد ISO/IEC 12207 از جمله فرایند امحای نرم‌افزار هستند.

#### ۸-۱-۲-۷-۱۲ تخریب

فعالیت‌های تخریب در تخریب امن تمام اطلاعات برنامه کاربردی از جمله داده‌های کاربر، اطلاعات سازمان، ثبت ورود و خروج کاربر و پارامترهای کاربردی و غیره دخالت دارند. این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای در سطح سازمان اجرا می‌شوند و دربرگیرنده فرایندهای مهندس نرم‌افزار از استاندارد ISO/IEC 12207 از جمله فرایند امحای نرم‌افزار هستند.

#### ۸-۱-۲-۷-۱۳ مدیریت زیرساخت تأمین برنامه کاربردی

این قسمت از فعالیت‌ها در مرحله تأمین شامل فعالیت‌های مرتبط با تهیه و نگهداری یک زیرساخت فناوری امن در پشتیبانی از فعالیت‌های تیم تأمین است و شامل فعالیت‌ها، امکانات، ابزارها و ارتباطات و دارایی‌های فناوری اطلاعات در محیط توسعه و محیط‌های آزمایش گوناگون هستند. این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای در سطح سازمان اجرا شده و دربرگیرنده فرایندهای مهندس نرم‌افزار از استاندارد ISO/IEC 12207 از جمله فرایند مدیریت زیرساخت و فرایند مدیریت پیکر-بندی است.

#### ۸-۱-۲-۷-۱۴ مدیریت زیر ساخت عملیات برنامه کاربردی

این قسمت از فعالیت‌ها در مرحله تأمین شامل فعالیت‌های شامل شده در تهیه و نگهداری یک زیرساخت فناوری امن برای مراحل عملیاتی چرخه حیات یک برنامه کاربردی است و دربرگیرنده خدمات، امکانات، ابزارها و ارتباطات و دارایی‌های فناوری اطلاعات در محیط عملیاتی برنامه کاربردی هستند. فعالیت‌های دیگر باید در طی مراحل عملیات جهت نگهداری امن زیرساخت پشتیبان برنامه انجام شوند. نگهداری زیر ساخت شامل نگهداری سامانه و سخت‌افزار شبکه، نسخه پشتیبانی و بازیابی، بازیابی پس از بحران و غیره است.

اینگونه فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای در سطح سازمان اجرا شده و دربرگیرنده فرایندهای مهندسی سامانه استاندارد ISO/IEC 5288 از جمله فرایند عملیات و فرایند نگهداری هستند.

#### ۸-۱-۲-۷-۱۵ امحا

فعالیت‌های امحای برنامه کاربردی جهت ارائه تضمین اینکه اطلاعات ذخیره‌شده بر روی سرورها، سامانه‌ها و سایر اجزای فنی مورد استفاده یک برنامه کاربردی به شکل امن پاک شده‌اند، اجرا می‌شوند. این امر اجازه می‌دهد سازمان بدون مخاطرات امنیتی این اجزا را امحا یا بازیافت کند. این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای سطح سازمانی اجرا می‌شوند و شامل فرایندهای مهندسی سامانه استاندارد ISO/IEC 5288 از قبیل فرایند امحا هستند.

#### ۸-۱-۲-۷-۱۶ تأمین ممیزی برنامه کاربردی

فعالیت‌های ممیزی بر کلیه فعالیت‌ها، کنش‌گرها، فرایندها، محصولات و اجزای برنامه کاربردی که در طی چرخه حیات برنامه کاربردی استفاده یا تولید می‌شوند، اعمال می‌گردند.

این فعالیت‌ها براساس سطح اعتماد هدف‌گذاری شده پروژه برنامه کاربردی ممکن است یک بار یا به صورت دوره‌ای توسط تیم‌های ممیزی داخلی یا خارجی اجرا شوند و به مالک برنامه کاربردی این اطمینان را می‌دهند که نیازهای امنیتی برنامه کاربردی در حد انتظار برآورده شده است.

فعالیت‌های ممیزی اجرا شده در مرحله تأمین معمولاً با مرحله عملیات تفاوت دارند. سازمان‌هایی که برنامه تولید کرده ولی اجرا نمی‌کنند، (مانند فروشندگان نرم‌افزار) شاید هرگز نیاز به ممیزی برنامه در مرحله عملیات نداشته باشند. به همین دلیل مدل ارجاعی چرخه حیاتی امنیتی برنامه، محدوده ویژه‌ای برای فعالیت‌های ممیزی در طی مراحل تأمین ارائه می‌کند.

این فعالیت‌ها معمولاً به عنوان قسمتی از فرایندها در سطح سازمان اجرا شده و دربرگیرنده فرایندهای مهندسی نرم‌افزار از استاندارد ISO/IEC 12207، از جمله فرایند ممیزی نرم‌افزار هستند.

#### **۸-۱-۲-۷-۱۷ ممیزی عملیات برنامه کاربردی**

فعالیت‌های ممیزی در طی مراحل عملیات برنامه کاربردی معمولاً مراحل تأمین تفاوت دارند. سازمان‌هایی که با برنامه‌های کسب‌شده کار می‌کنند، ممکن است نیاز به ممیزی برنامه کاربردی در مراحل تأمین نداشته باشند و به همین دلیل مدل مرجع چرخه حیات امنیت برنامه کاربردی، محدوده ویژه‌ای برای فعالیت‌های ممیزی در طی مراحل عملیات ارائه می‌کند.

این فعالیت‌ها معمولاً به عنوان قسمتی از فرایندها در سطح سازمان اجرا شده و دربرگیرنده فرایندهای مهندسی نرم‌افزار استاندارد ISO/IEC 12207 از جمله فرایند ممیزی برنامه کاربردی هستند.

#### **۸-۱-۲-۸ فرایندهای مربوط به امنیت برنامه کاربردی**

ONF انبار کلیه فرایندهای مورد استفاده سازمان است. بنابراین کلیه فرایندهای مربوط به تعریف مدیریت و تأیید صلاحیت امنیت برنامه کاربردی باید به‌طور رسمی در ONF توصیف شوند. از جمله:

الف) تمام فرایندهای توصیف شده در بند ۸ این استاندارد ملی

ب) تمام فرایندهای تعریف شده در قسمت‌های بعدی استاندارد ISO/IEC 27034

پ) تمام فرایندهایی که در ASC‌هایی مانند طرح‌های واکنش به حادثه، طرح‌های ادامه فعالیت کسب و کار، روش‌های بازبینی کد و روش‌های آزمایش آسیب‌پذیری به آنها مراجعه شود.

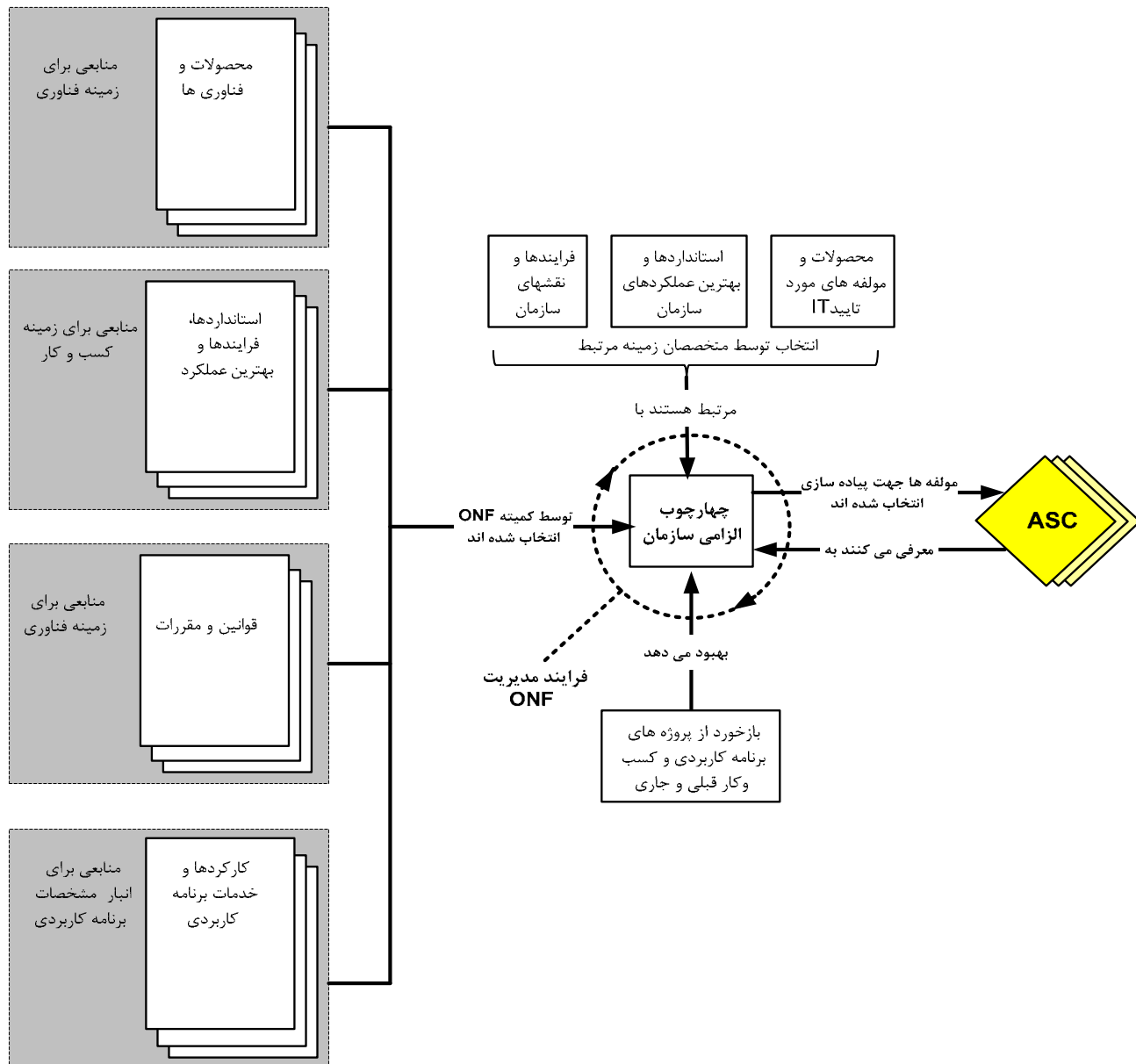
#### **۸-۱-۳ فرایندهای مربوط به چارچوب الزامی سازمان**

##### **۸-۱-۳-۱ کلیات**

زمینه سازمانی در طول زمان تکامل می‌یابد، به همین دلیل اجزای ONF معرف این زمینه‌ها مانند زمینه فنی، کسب و کار و مقررات تنظیم شده و خصوصیات برنامه کاربردی باید به‌روز باشند. کمیته ONF باید فرایندهای ایجاد، تأیید و نگهداری ONF و تمام اجزای آن را تعریف، ثبت و تصویب کند. جایگاه‌ها مسئولیت‌پذیری‌ها و صلاحیت‌های حرفه‌ای کنش‌گرهای درگیر در جریان فرایندها نیز باید مشخص شود. به عنوان مثال شکل ۹ نمای کلی از فرایند نگهداری ONF را نشان می‌دهد.

این فرایندها در شمای کلی حاضر ارائه شده و به تفصیل در استاندارد ISO/IEC 27034-2 مورد بحث قرار خواهند گرفت.

## ۸-۱-۳-۲ فرایند مدیریت ONF



شکل ۹- فرایند مدیریت ONF

فرایند مدیریت ONF (شکل ۹) و فرایندهای فرعی آن، فرایندهای دائمی هستند که توسط کمیته ONF انجام می‌پذیرند. این فرایندها مستقل از پروژه‌های برنامه کاربردی سازمان بوده و همان‌طور که در شکل ۳ نشان داده شده، به‌طور موازی با آنها اجرا می‌شوند. اهداف فرایند مدیریت ONF عبارتند از :



الف) تضمین اینکه نیازهای امنیتی برنامه‌های کاربردی و تأیید کتابخانه ASC و سطح اعتماد به‌ویژه سطح اعتماد صفر با نیازهای کسب و کار سازمان همسو هستند.

ب) تضمین اینکه مولفه‌های ONF جهت بازتاب تغییرات واقع‌شده در خارج از سازمان به‌روز هستند. به‌عنوان مثال تغییر در قوانین می‌تواند باعث تغییر زمینه مقررات تنظیم‌شده در ONF شود.

پ) کسب تاییدیه از مدیران عالی درمورد سیاست‌های امنیتی در سطح سازمان و مدیران ارشد در مورد اهمیت تمامی مولفه‌های ONF

ت) تضمین اینکه ASC‌های تأییدشده به‌طور مناسب و یکنواخت در سطح سازمان اعمال می‌شوند.

ث) ارسال اجزای ONF به تمام تیم‌ها در سازمان

ج) ارائه بازخورد به ONF جهت پوشش دانش جدید پیشنهادات، در مورد پیشرفت ASC روش‌های جدید به‌دست آمده در طول یک پروژه برنامه کاربردی

#### ۸-۱-۳ فرایندهای فرعی مدیریت ONF

تمامی فرایندهای مرتبط به امنیت برنامه‌های کاربردی باید با قسمتی از ONF یا ISMS سازمان نیز مطابقت داشته باشند. جدول زیر نشان می‌دهد که چگونه فرایندهای فرعی مدیریت ONF مرتبط با امنیت برنامه کاربردی با چهار وضعیت فرایند ISMS هم جهت می‌شوند.

جدول ۲- تطابق ISMS و فرایندهای فرعی مدیریت ONF مرتبط با امنیت برنامه کاربردی

فرایند فرعی مدیریت ONF	فرایند ISMS
طراحی ONF	طرح
پیاده‌سازی ONF	اجرا
نظارت و بازبینی ONF	بررسی
پیشرفت مداوم ONF	اقدام

همان‌گونه که در جدول ۲ نشان داده شده، فرایند مدیریت ONF می‌تواند به چهار فرایند فرعی تقسیم شود:

**الف) طراحی ONF :**

- ۱- مشخص کردن و ثبت تمامی زمینه‌های ممکن (کسب و کار، مقررات تنظیم‌شده و فنی) که برنامه کاربردی در آنها مورد استفاده قرار خواهد گرفت.
- ۲- ایجاد ثبت و نگهداری انباره مشخصات برنامه کاربردی
- الف) تحلیل مشخصات هر برنامه کاربردی جدید در طی مرحله تهیه
- ب) تحلیل مشخصات برنامه‌های کاربردی موجود در سازمان
- ۳- مشخص کردن کنش‌گرها و فرایندها

الف) تحلیل و ثبت افراد و فرایندهای درگیر در چرخه حیات برنامه کاربردی

ب) مشخص کردن و تأیید روشگان تحلیل مخاطره در سطح برنامه کاربردی رسمی براساس استاندارد ملی

۲۷۰۰۵

۴- تحلیل بهترین تجارب و استانداردها مانند استاندارد ISO/IEC 12207 ، استاندارد ISO/IEC 5288 ، استاندارد ISO/IEC 15026 و تعریف ASCها براساس این تحلیل:

الف) ایجاد و بهروزرسانی ASC

در هنگام نیاز سازمان، یک ASC جهت رسیدگی به یک نیاز امنیتی ویژه ایجاد یا بهروزرسانی می‌شود. بهتر است متخصصین زمینه‌ها فعالیت‌های امنیت و سنجش درستی‌سنجی را همان‌گونه که در زیربند ۸-۱-۲-۶-۵ مطرح‌شده تعیین کنند.

مثال ۱- یک ASC مورد نیاز جهت اعمال امنیت برنامه کاربردی که باید توسط برنامه‌ریزی ارشد و با کفایت در یک زبان برنامه‌نویسی ویژه ایجاد یا بهروزرسانی شود.

مثال ۲- یک ASC مورد نیاز جهت اعمال یک فرایند مدیریت هویت برنامه باید توسط یک متخصص مدیریت هویت ایجاد یا بهروزرسانی شود.

ب) اعتبارسنجی و یکپارچه‌سازی ASC

توصیه می‌شود تیم درستی‌سنجی متشکل از مدیران ارشد و تدوین‌گران متخصص، کارکنان و بازرسان فناوری اطلاعات مسئول اعتبار سنجی یک ASC بوده و ضمانت کنند که این ASC برای کاربران قابل فهم خواهد بود و نیز تأیید کنند که این ASC در واقع مخاطره تعریف‌شده را کاهش می‌دهد. همچنین توصیه می‌شود تیم مذکور مشخص کنند این ASC برای کدام سطح اعتماد لازم است.

تأیید نهایی ASCها مسئولیت کمیته ONF است

۵- تحلیل مقایسه با مدل مرجع چرخه حیات امنیت برنامه کاربردی و الزاماً تنظیم مدل چرخه حیات برنامه کاربردی حال حاضر سازمان و سایر فرایندها

۶- تعریف و پیاده‌سازی کتابخانه ASC برنامه کاربردی

۷- اکتساب (یا تدوین) بهروزرسانی و اعتبارسنجی ASCهای مورد نیاز سازمان و یکپارچه‌سازی آنها در کتابخانه ASC

۸- تحلیل، تنظیم و درستی‌سنجی بازخورد پروژه برنامه کاربردی

ب) پیاده‌سازی ONF: پیاده‌سازی و برقراری ارتباط ONF

پ) پایش و بازبینی ONF: تضمین استفاده صحیح از ONF در پروژه‌های برنامه کاربردی و جمع‌آوری بازخورد از این پروژه‌ها:

۱- نیازمند یک سطح اعتماد هدف‌گذاری‌شده و یک سطح اعتماد واقعی برای تمام برنامه‌های کاربردی مورد استفاده سازمان است.

۲- نیازمند ارزیابی مخاطره برنامه کاربردی به‌صورت دوره‌ای برای تمامی برنامه‌های کاربردی مورد استفاده سازمان است.

ت) پیشرفت مداوم ONF: نگهداری و پیشرفت اجزای ONF از طریق بازبینی دوره‌ای زمینه‌ها در سطح سازمان، افراد و فرایندها و فناوری یافتن تمام تغییراتی که ممکن است بر ASMP تأثیرگذار باشند و یکپارچه‌سازی آنها در ONF.

## ۸-۲ ارزیابی مخاطره امنیت برنامه کاربردی

### ۸-۲-۱ ارزیابی مخاطره در مقابل مدیریت مخاطره

ارزیابی مخاطره، مرحله دوم فرآیند مدیریت مخاطره است که در استاندارد ملی ۲۷۰۰۵ توضیح داده شد. به این ترتیب، ارزیابی مخاطره امنیت برنامه کاربردی، مرحله دوم فرآیند مدیریت امنیت برنامه کاربردی است و فرآیند ارزیابی مخاطره را در سطح برنامه کاربردی اجرا می‌کند. دیگر مراحل مدیریت مخاطره توسط دیگر مراحل فرآیند مدیریت امنیت برنامه کاربردی به اجرا در می‌آیند.

مطابق استاندارد ملی ایران به شماره ۲۷۰۰۵، «ارزیابی مخاطره ارزش اطلاعاتی سرمایه، هویت تهدیدها و آسیب‌پذیری‌های موجود یا محتمل را مشخص می‌کند، نظارت‌های موجود و تأثیر آنها را بر مخاطره‌های تعیین‌شده نشان می‌دهد، نتایج بالقوه را نمایان می‌سازد و در نهایت مخاطره‌های مشتق شده را الویت‌بندی می‌کند و آنها را براساس معیار ارزیابی مخاطره موجود در زمینه سازمان رتبه‌بندی می‌کند.» ارزیابی مخاطره خود سه مرحله دارد: تعیین مخاطره، تحلیل مخاطره و ارزشیابی مخاطره

### ۸-۲-۲ تحلیل مخاطره برنامه کاربردی

#### ۸-۲-۲-۱ تحلیل مخاطره سطح بالای برنامه کاربردی

در مرحله آماده‌سازی چرخه برنامه کاربردی، یک تحلیل مخاطره سطح بالا اجرا می‌شود. این تحلیل، بر پایه مشخصات برنامه کاربردی و زمینه‌های فنی، مقررات تنظیم‌شده و کسب و کار سطح هدف‌گذاری‌شده را تعریف می‌کند.

توصیه می‌شود مالک پروژه برنامه کاربردی خاص جایگاه مشخصی برای مسئولیت اجرای این تحلیل و با استفاده از روشی مناسب برای تحلیل سطحی برنامه کاربردی مشخص کند. روش تحلیل مخاطره سطح سازمانی نباید به این یک وظیفه ختم شود.

#### ۸-۲-۲-۲ تحلیل مخاطره تفصیلی برنامه کاربردی

این تحلیل در مرحله تحقق چرخه حیات برنامه کاربردی اجرا می‌شود و به شکل دقیق، مخاطرات دیگر مرتبط با برنامه کاربردی را قبل از تعیین امنیت برنامه مشخص می‌کند و سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی را با توجه به مشخصات برنامه کاربردی، زمینه فنی و مقررات تنظیم‌شده برای برنامه کاربردی در سازمان مورد نظر تأیید می‌کند.

در پی این تحلیل مخاطره مفصل، ممکن است مالک برنامه کاربردی سطح اعتماد ایده‌آل برنامه کاربردی را برای پروژه کاربری تغییر دهد. این مسئله، کنترل امنیت برنامه انتخاب‌شده برای پروژه را تغییر می‌دهد و به همین ترتیب بر عوامل درگیر و هزینه‌ی برآورد شده تأثیر می‌گذارد. با این وجود، به دلیل دسترسی به اطلاعات مربوط به عوامل، توانایی‌های تخصصی و برآورد هزینه در کنترل امنیت برنامه سازمان، این تأثیرات به آسانی قابل پیش‌بینی هستند.

مالک پروژه‌های خاص کاربردی باید مسئولیت خاصی برای اجرای این تحلیل و استفاده از روش‌های مناسب برای تحلیل در سطح برنامه در نظر گیرند. روشگان ارزیابی مخاطره در سطح سازمانی برای این فعالیت مناسب نخواهد بود.

#### ۸-۲-۳ ارزیابی مخاطره

طبق استاندارد ملی ایران به شماره ۲۷۰۰۵، «ارزیابی مخاطره، با استفاده از درکی که تحلیل مخاطره از مخاطرات فراهم آورده است، نسبت به اقدامات آینده تصمیم می‌گیرد. این تصمیمات باید شامل موارد زیر باشند:

الف) لزوم اجرای یک فعالیت

ب) اولویت‌های برطرف سازی مخاطره با در نظر گرفتن سطوح برآورد شده مخاطرات.»

این مرحله در این استاندارد شکل سطح اعتماد هدف‌گذاری شده را می‌گیرد که خود تعیین می‌کند کدام یک از کنترل‌های امنیت برنامه کاربردی باید برای حل مخاطره به کار گرفته شوند.

#### ۸-۲-۴ سطح اعتماد هدف‌گذاری شده برنامه کاربردی

سطح اعتماد هدف‌گذاری شده برنامه کاربردی می‌تواند در دستیابی به سطح اعتماد مورد نظر سازمان کمک کند تا برنامه پس از پذیرفته شدن مخاطرات مشخص شده در ارزیابی مخاطره به شیوه‌های امن مورد استفاده قرار گیرد.

سطح اعتماد هدف‌گذاری شده برنامه کاربردی در زمینه امنیت برنامه بسیار حیاتی است و این به دلیل دخالت مستقیم آن در تعیین کنترل امنیت برنامه کاربردی مناسب از کنترل امنیت برنامه کاربردی و پیاده‌سازی آن در چرخه حیات برنامه کاربردی است.

فرآیند ارزیابی مخاطره، نیازهای امنیتی را مطرح می‌کند که سطح اعتماد هدف‌گذاری شده برنامه کاربردی از آنها مشتق می‌شوند. سطح اعتماد هدف‌گذاری شده برنامه کاربردی خود هدف گروه پروژه برنامه کاربردی می‌شود.

سطح اعتماد ایده‌آل برنامه باید یکی از سطوح اعتمادی باشد که در گنجینه سازمانی کنترل امنیت برنامه تعریف شده است.

گنجینه کنترل امنیت برنامه (شکل ۵) را می‌توان به شکل جدولی نشان داد که سطح اعتماد ایده‌آل برنامه، ستون‌های آن هستند. به این ترتیب انتخاب یک سطح اعتماد، گزینش تمام کنترل امنیت برنامه‌های موجود در آن ستون را به دنبال خواهد داشت.

#### ۸-۲-۵ پذیرش مالک برنامه کاربردی

مالک برنامه کاربردی مسئولیت پذیرش مخاطرات مرتبط با برنامه کاربردی مورد بررسی را دارد.

مالک برنامه کاربردی می‌تواند به دو صورت این پذیرش را اعلام کند:

الف. تأیید سطح اعتماد هدف‌گذاری شده برنامه کاربردی در مرحله دوم فرایند مدیریت امنیت برنامه کاربردی

ب. تأیید نتایج ممیزی امنیت برنامه کاربردی در مرحله پنجم فرایند مدیریت امنیت برنامه کاربردی که طی آن سطح اعتماد واقعی برنامه سنجیده و با سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی مقایسه می‌شود. این مرحله می‌تواند در هر زمانی توسط مالک برنامه کاربردی درخواست شود. مالک برنامه کاربردی می‌تواند گروهی خارجی را برای درستی سنجی بیشتر درخواست کند. پس از اجرای پذیرش توسط مالک برنامه کاربردی، مسئولیت دستیابی به سطح اعتماد هدف‌گذاری‌شده با پیاده‌سازی کنترل امنیت برنامه کاربردی مرتبط در مراحل مناسب چرخه حیات برنامه کاربردی بر عهده گروه پروژه است.

### ۸-۳ چارچوب الزامی برنامه کاربردی

#### ۸-۳-۱ کلیات

چارچوب الزامی برنامه کاربردی (ANF) زیرمجموعه یا شکل تصحیح‌شده چارچوب الزامی سازمان است که فقط اطلاعات جزئی مورد نیاز برنامه کاربردی خاص را برای رسیدن به سطح اعتماد هدف‌گذاری‌شده توسط مالک برنامه کاربردی در جریان عنصر فرایند پذیرش گام دوم ASMP شامل می‌شود. الزامات امنیتی ANF از ارزیابی مخاطراتی مشتق می‌شوند که مربوط به استفاده سازمان از برنامه کاربردی اجراشده در گام دوم ASMP هستند. برای هر پروژه برنامه کاربردی، ANF مرتبط با زمینه‌های فنی، مقررات تنظیم شده و کسب و کار، مشخصات برنامه کاربردی و ASCها ایجاد و کامل می‌شود. این ANF در جریان چرخه حیات برنامه کاربردی وجود دارد و می‌تواند در طول زمان تکمیل شود. برای مثال، زمینه مقررات تنظیم‌شده برنامه کاربردی می‌تواند در جریان پروژه تغییر کند یا ممکن است مالک برنامه کاربردی به گروه پروژه برنامه کاربردی، سطح اعتماد هدف‌گذاری‌شده جدیدی بدهد. در چنین مواردی، ممکن است عناصر جدیدی توسط سازمان به ANF اضافه یا از آن حذف شوند. تغییرات ANF بر امنیت برنامه کاربردی اثر می‌گذارد. این تغییرات باید تأییدیه‌های مربوطه را از مالک برنامه کاربردی دریافت کنند. ANF پروژه برنامه کاربردی خاص اجزای تفصیلی زیر را شامل می‌شود. شکل ۱۰ نمایش نموداری ANF است.



شکل ۱۰- چارچوب الزامی برنامه کاربردی

#### ۸-۳-۲ مولفه‌ها

##### ۸-۳-۲-۱ زمینه کسب و کار مربوط به محیط برنامه کاربردی

تمام فرآیندهای کسب و کار، روش‌ها، استانداردها و کنش‌گرهای درگیر در پروژه برنامه کاربردی، اعم از فرآیندهای کسب و کار خارجی مورد نیاز برای فراهم‌آوردن یکپارچگی کسب و کار مناسب در محیط اجرایی از زمینه کسب و کار ONF سازمان (به زیربند ۸-۳-۱-۲-۱ مراجعه شود). مشتق و براساس آن تصحیح می‌شوند.

##### ۸-۳-۲-۲ زمینه مقررات تنظیم شده مربوط به محیط برنامه کاربردی

تمام الزامات قانونی و مقررات تنظیم‌شده قابل کاربری در جایی که برنامه مورد استفاده مفید قرار می‌گیرد از زمینه مقررات تنظیم‌شده ONF سازمان (به زیربند ۸-۳-۱-۲-۲ رجوع کنید). مشتق و براساس آن تصحیح می‌شوند.

##### ۸-۳-۲-۳ زمینه فنی مربوط به محیط برنامه کاربردی

تمام اجزای فنی برنامه کاربردی از قبیل معماری، زیرساخت، پروتکل‌ها و زبان‌ها از زمینه فنی ONF سازمان (به زیربند ۸-۳-۱-۲-۴ مراجعه شود). مشتق و براساس آن تصحیح می‌شوند.

#### ۸-۳-۲-۴ مشخصات برنامه کاربردی

ویژگی‌های برنامه به سه شکل کارکردی، غیر کارکردی و الزامات امنیتی در می‌آیند. تمام داده‌هایی که استفاده، ذخیره، محاسبه، به اشتراک گذاشته و منتقل می‌شوند، بایستی فهرست و طبقه‌بندی شوند. این مسئله داده‌های سازمانی، داده‌های کاربران، داده‌های تنظیمی، پارامترها و دیگر داده‌های استفاده شده توسط برنامه کاربردی را شامل می‌شود. این امر در مورد داده‌های خروجی برنامه نیز صدق می‌کند.

#### ۸-۳-۲-۵ کنش‌گرهای برنامه کاربردی: جایگاه‌ها، مسئولیت‌پذیری‌ها و صلاحیت‌ها

تمام عواملی که با برنامه کاربردی و در جریان چرخه حیات برنامه کاربردی با برنامه کاربردی در ارتباط هستند باید مشخص شوند. کنش‌گرها شامل: کارکنان امنیتی، مالکان برنامه کاربردی، مدیران پروژه، کارکنان ممیزی، معماران، آزمایش‌دهندگان، توسعه‌دهندگان، کاربران نهایی، سرپرست‌ها، سرپرست‌های دادگان و منحصان فناوری می‌شوند.

#### ۸-۳-۲-۶ ASCهای برگزیده چرخه حیات امنیت برنامه کاربردی

همان‌گونه که در زیربند ۸-۱-۲-۶ دیده می‌شود، ASCهای دقیق و مفصل هر پروژه برنامه کاربردی خاص از کتابخانه ASCهای سازمان و براساس معیارهای زیر انتخاب می‌شوند:

الف) سطح اعتماد هدف‌گذاری شده برنامه کاربردی

ب) الزامات سازمان برای برنامه کاربردی

پ) زمینه و مشخصات خاص برنامه کاربردی

هر ASC همزمان فعالیت امنیتی را فراهم می‌آورد که توسط گروه پروژه برنامه کاربردی اجرا می‌شود تا مخاطره امنیتی خاصی را کاهش دهد و همزمان سنجش درستی، آزمون درستی‌سنجی را به اجرا در می‌آورند تا با بررسی شواهد اثباتی تأیید کنند فعالیت امنیتی مرتبط با موفقیت اجرا شده است. همچنین ASC نشانه‌هایی را برای مراحل خاصی از چرخه حیات برنامه کاربردی که فعالیت و سنجش مورد نظر باید در آن صورت گیرد، فراهم می‌کند.

ASC توسط سازمان و پیش از توسعه تعریف و تأیید می‌شود. لازم نیست توسعه‌دهندگان برای هر پروژه برنامه کاربردی آنها را طراحی کنند. این رهیافت مداوم سازمان را در برخورد با الزامات امنیتی برنامه کاربردی تأیید می‌کند.

ASCهای برگزیده باید حداقل شامل تمام ASCهایی باشد که کمیته ONF برای سطح اعتماد صفر تصویب کرده است. گروه پروژه نباید در جریان پروژه برنامه کاربردی، ASCهای تصویب شده برای سطح اعتماد صفر را تغییر دهند.

### ۸-۳-۳ فرآیندهای مرتبط با امنیت برنامه کاربردی

مطابق این استاندارد ملی، ANF باید تمام فرآیندهای مرتبط با تعریف، مدیریت و درستی سنجی امنیت برنامه کاربردی را شامل شود. این مسئله، همان گونه که در زیربند ۸-۲-۱-۸ توصیف شده، تصحیح جز «فرآیندهای مربوط به امنیت برنامه کاربردی» ONF است.

### ۸-۳-۴ چرخه حیات برنامه کاربردی

چرخه حیات برنامه کاربردی مراحل و فعالیت های برگزیده از ONF را برای پروژه برنامه کاربردی خاصی به تصویر می کشد. به طور دقیق تر، چرخه حیات برنامه کاربردی زیرمجموعه ای از مدل مرجع چرخه حیات امنیت برنامه کاربردی است. (به زیربند ۸-۲-۱-۷ مراجعه شود). در مورد چرخه حیات برنامه کاربردی و همتای استاندارد آن، مدل مرجع چرخه حیات امنیت برنامه کاربردی، پیش تر در زیربند ۸-۲-۱-۷ صحبت شد. سنجش ها و فعالیت های تعریف شده توسط ASC، از طریق فرآیندهای متنوعی که در چرخه حیات برنامه کاربردی استفاده می شوند و گروه پروژه و درستی سنجی با آنها آشنا هستند، اجرا می شوند. به این ترتیب یکپارچگی تدریجی ASC ها به عنوان فرآیندهای یکپارچه استفاده شده در چرخه حیات برنامه کاربردی نسبت به فعالیت های امنیتی خارجی مجزا ارجحیت دارد.

### ۸-۳-۵ فرآیندها

#### ۸-۳-۵-۱ فرآیندهای مرتبط با چارچوب الزامی برنامه کاربردی

سازمان باید فرآیندهای ایجاد، تأیید و نگهداری ANF را تعریف و ثبت کند. جایگاه ها، مسئولیت ها و صلاحیت های حرفه ای مورد نیاز عوامل درگیر در ANF برنامه کاربردی خاص باید مشخص شوند. فرآیند ایجاد ANF برنامه کاربردی خاص، فرآیندی حیاتی است. این فرآیند اطلاعات کلی موجود در ONF را به اطلاعات خاص مورد نیاز ANF برنامه کاربردی خاص و الزامات آن تبدیل می کند. در حالی که ASC های موجود در ONF به مراحل مدل مرجع چرخه حیات امنیت برنامه کاربردی متصل هستند، ASC های ONF به مراحل چرخه حیات برنامه کاربردی خاص متصل هستند.

#### ۸-۳-۵-۲ فرایند بازخورد

سازمان باید فرآیندی را برای بهبود دائم ONF از طریق بازخورد دانش جدید، پیشنهادهای بهبود کنترل امنیت برنامه کاربردی و روش های به دست آمده در زمان توسعه و استفاده مفید از برنامه کاربردی، تعریف کند.

این فرآیند در شکل ۳ با عنوان «بازخورد فراهم شده» نشان داده شده است.

این فرآیند باید با فرآیند نگهداری ANF که در شکل ۹ با عنوان «بازخوردهای کسب و کار پیشین و جاری و پروژه های برنامه کاربردی» نشان داده شده است، تلفیق شود.



## ۸-۴ فراهم کردن مقدمات و اجرای برنامه کاربردی

### ۸-۴-۱ کلیات

مرحله چهارم ASMP شامل استفاده مفید و پیگیری در پروژه برنامه کاربردی ASC های خاص می شود که توسط ANF فراهم شده است. گروه پروژه کاربری به طور خاص فعالیت های امنیتی خاص توصیف شده در قسمت «فعالیت امنیتی» ASC را (همان گونه که در زیربند ۸-۱-۲-۳-۴-۵ توضیح داده شده است) برای هر ASC موجود در AFN پیاده سازی می کند.

این مرحله برای گروه پروژه و گروه درستی سنجی، با فراهم آوردن ASC های مورد نیاز برای دستیابی به سطح اعتماد هدف گذاری شده آسان تر می شود. نیازی نیست که گروه ها از فرآیندهایی که به ANF ها منجر می شوند آگاه باشند.

ASC برای مدیران پروژه ابزار مفیدی خواهد بود. کنترل امنیت برنامه وظایف، منابع و صلاحیت های مورد نیاز، هزینه هر وظیفه بر پایه روز- فرد و دقیقاً مرحله ای از چرخه حیات که فعالیت باید در آن صورت بگیرد را به طور مفصل شرح می دهد.

ASC برای گروه درستی سنجی نیز ابزاری مفید خواهد بود زیرا اطلاعات دقیق مربوط به این که چه نوع درستی سنجی باید اجرا شود تا ثابت کند فعالیت های امنیتی اجرا شده و دستیابی به نتایج مورد نظر مناسب است را فراهم می کند. این مسئله کمک می کند، گروه سنجش صحت از مطابقت برنامه کاربردی با نیازهای امنیتی اعتماد حاصل کنند.

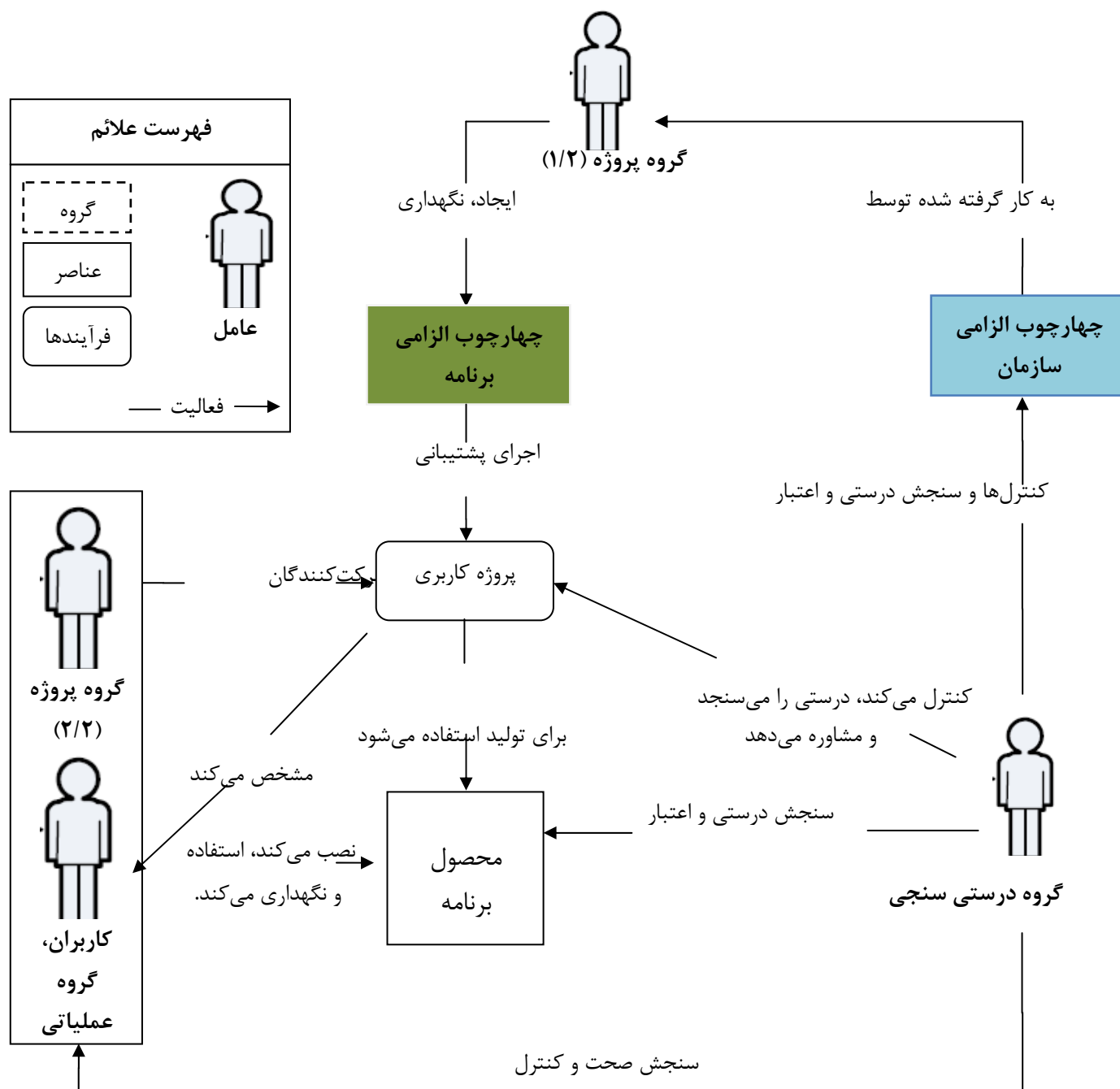
ASC برای گروه های امنیتی و فنی نیز مفید خواهد بود زیرا ASC موجود در ANF خاص فهرست مفصلی از الزامات امنیتی را ارائه می دهد و به این شکل برنامه ریزی پیشرفته منابع مورد نیاز را ممکن می سازد.

### ۸-۴-۲ تأثیر استاندارد ISO/IEC 27034 بر یک پروژه برنامه کاربردی

هر پروژه برنامه کاربردی معمول (پیش از پیاده سازی استاندارد ISO/IEC27034) توسط گروه پروژه، با پشتیبانی فرایندها و خودکار شدن توسط فناوری با هدف ایجاد یک برنامه هدایت می شود. اغلب، گروه تضمین کیفیت برنامه کاربردی، برنامه آزمایش را برای درستی سنجی کارکردهای برنامه کاربردی در مقابل الزامات کارکردی مورد پذیرش دنبال می کنند.

خود فناوری، روش های مورد استفاده گروه پروژه، تکمیل فرآیند، کیفیت محصولات مصنوعی تولید شده و کیفیت کنش گرهای درگیر در پروژه به ندرت درستی سنجی می شوند و چنانچه فرآیند درستی سنجی اجرا شود به شکل رسمی تعریف نمی شوند.

شکل ۱۱ چگونگی تأثیر استاندارد ISO/IEC27037 در اضافه کردن جایگاه ها، مسئولیت پذیری ها، اجزا و فرآیندها را در یک پروژه برنامه کاربردی نشان می دهد.



شکل ۱۱ چگونگی چگونگی مشخص کردن رسمی جایگاه‌ها و مسئولیت‌پذیری‌ها را نشان می‌دهد. همچنین این شکل دو جزء جدید را به تصویر می‌کشد: ONF و ANF. ONF، چارچوبی گسترده در سازمان است که به‌طور مستقیم بر پروژه برنامه کاربری تأثیر نمی‌گذارد. گروه پروژه، گروه درستی‌سنجی و کاربران تنها تحت تأثیر ANF هستند، چارچوبی مختص هر برنامه کاربردی که کنترل‌های امنیت برنامه کاربردی دقیق و مفصلی مطابق با سنجش درستی ارائه می‌دهد.

گروه درستی‌سنجی مسئول درستی‌سنجی ONF است. این درستی‌سنجی تنها در سطح پروژه اجرا نمی‌شود (زیربند ۸-۴-۴-۲ را ببینید). بلکه در سطح سازمانی نیز به‌عنوان بخشی از فرایند ONF به اجرا در می‌آید. (زیربند ۸-۱-۳-۳-ت را ببینید).

#### ۸-۴-۳ مولفه‌ها

##### ۸-۴-۳-۱ گروه پروژه

گروه پروژه متشکل از افراد درگیر در پروژه برنامه کاربردی است که در مراحل فراهم آوردن مقدمات یا اجرای چرخه حیات برنامه کاربردی حضور دارند. از جمله مهندسان معمار، تحلیل‌گران، برنامه‌نویسان و آزمایشگران.

این افراد مسئول گزینش عناصر ONF برای ایجاد یا نگهداری ANF پروژه برنامه کاربردی هستند.

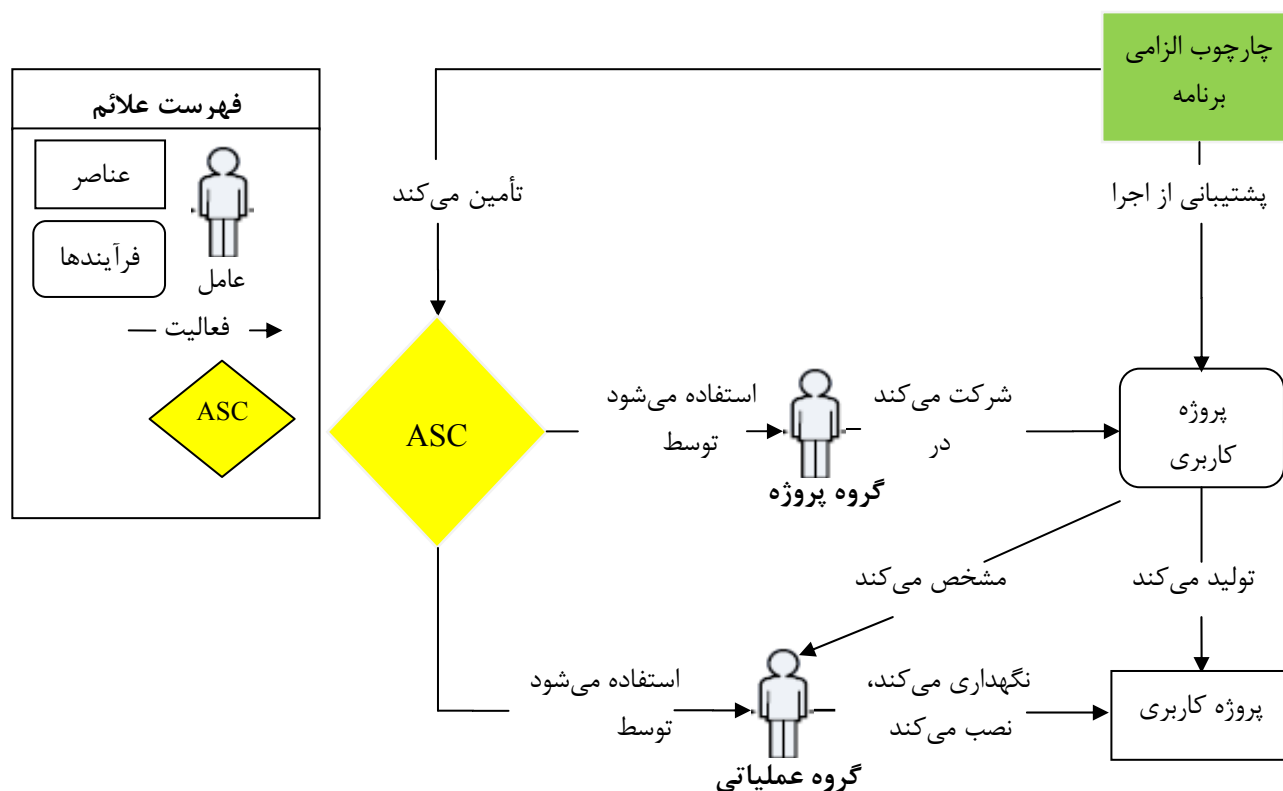
##### ۸-۴-۳-۲ گروه عملیاتی

گروه پروژه متشکل از افراد درگیر در مدیریت و نگهداری برنامه کاربردی است که در مراحل عملیاتی چرخه حیات برنامه کاربردی حضور دارند. از جمله سرپرستان سامانه، سرپرستان دادگان، سرپرستان شبکه و کارکنان فنی.

#### ۸-۴-۴ فرآیندها

##### ۸-۴-۴-۱ اجرای فعالیت‌های امنیتی در جریان یک پروژه کاربری

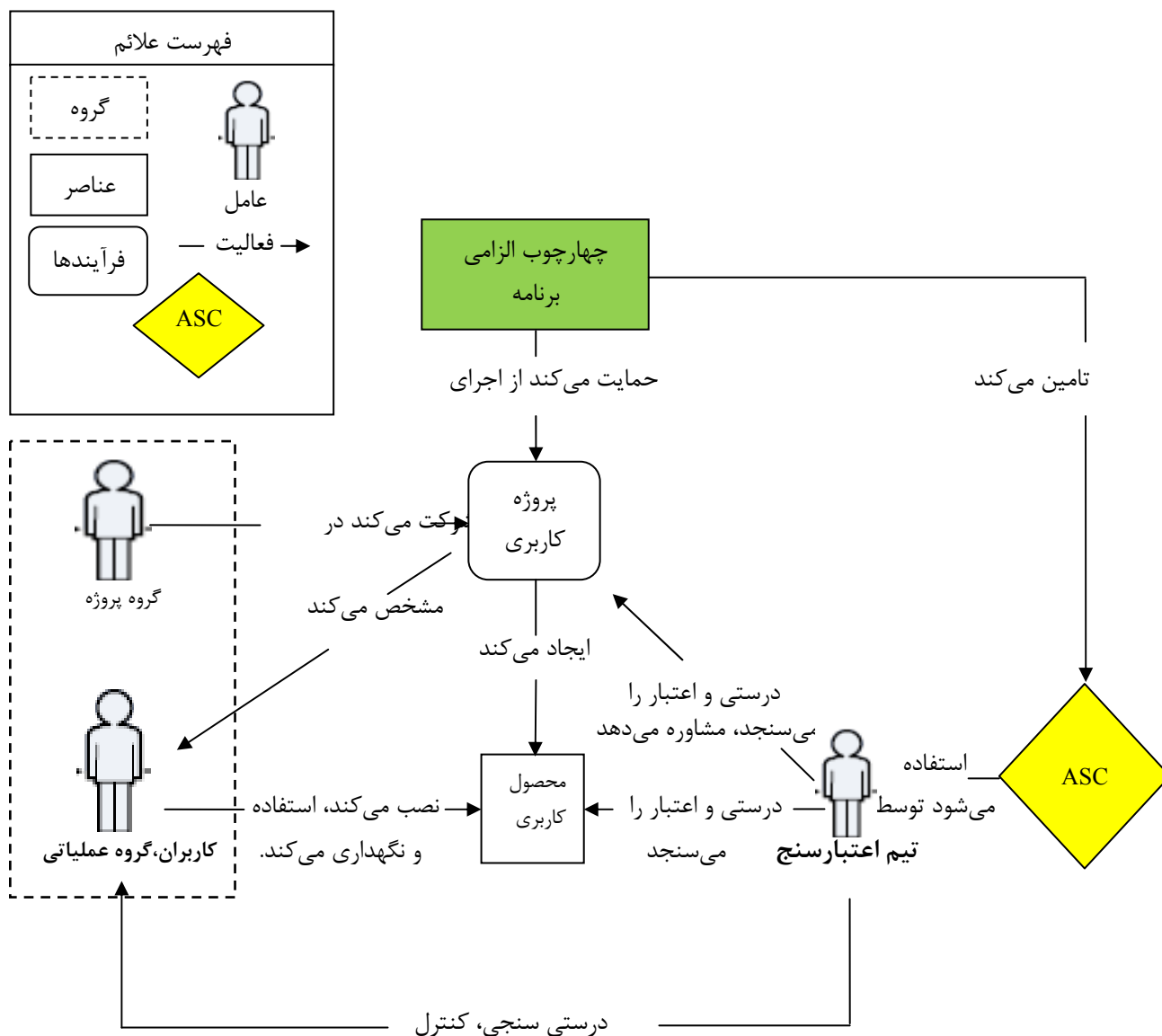
شکل ۱۲ نحوه استفاده گروه پروژه و گروه عملیاتی را از ASC به‌عنوان ابزاری برای اجرای فعالیت‌های امنیتی پروژه‌ای خاص نشان می‌دهد. فقط ASC موجود در ANF در این پروژه مورد استفاده قرار می‌گیرد.



شکل ۱۲- کنترل امنیت برنامه کاربردی به کار گرفته شده به عنوان فعالیت امنیتی

#### ۸-۴-۲ عملکرد سنجش درستی سنجی در جریان یک پروژه برنامه کاربردی

قسمت درستی سنجی ASC، اصولی را پیاده سازی می کند که بر اساس آنها تمام فعالیت های امنیتی باید درستی سنجی شوند تا بتوان اجرای صحیح فعالیت توسط عامل متخصص و دست یابی به نتایج مورد انتظار را در جریان ثابت کرد.



شکل ۱۳- کنترل امنیت برنامه کاربردی به کار گرفته شده به عنوان معیار سنجش

شکل ۱۳ نشان می دهد که قسمت درستی سنجی کنترل امنیت برنامه کاربردی به عنوان قسمت کنترلی در چرخه حیات برنامه کاربردی به کار گرفته می شود تا گروه درستی سنجی، برنامه و پروژه را سنجیده و مشاوره لازم را برای مالک برنامه کاربردی فراهم کند تا او بتواند نسبت به صدور مجوز حرکت به مرحله اجرایی بعدی تصمیم بگیرد. برای مثال، ممکن است ASC استفاده از خدمت خوشه بندی سرور را برای در دسترس بودن برنامه کاربردی لازم بداند. قسمت درستی سنجی ASC پیاده سازی صحیح این خدمت را کنترل کرده و می سنجد.

شکل ۱۳ همچنین نشان می دهد که درستی سنجی کنترل امنیت برنامه کاربردی می تواند برای تأیید صلاحیت های عوامل اجرایی فعالیت های چرخه حیات برنامه کاربردی مورد استفاده قرار گیرد. برای مثال، کنترل امنیت برنامه کاربردی ممکن است پیاده سازی یکی از اجزای حیاتی برنامه کاربردی را توسعه داده و

لازم بداند. سنجش صحت کنترل امنیت برنامه کاربردی، صلاحیت‌های توسعه‌گری را می‌سنجد تا این جزء را پیاده‌سازی کند.

## ۸-۵ ممیزی امنیتی برنامه کاربردی

### ۸-۵-۱ کلیات

هدف پنجمین فرآیند مدیریت امنیت برنامه کاربردی، سنجش درستی و ثبت رسمی این است که آیا برنامه کاربردی خاص به سطح اعتماد هدف‌گذاری شده دست یافته و آن را نگهداری می‌کند. این مرحله از فرآیند مدیریت امنیت برنامه کاربردی می‌تواند در هر زمانی در چرخه حیات برنامه کاربردی اجرا شود. بسته به سطح اعتماد هدف‌گذاری شده برنامه کاربردی این مرحله می‌تواند موردی، دوره‌ای یا موقعیتی باشد.

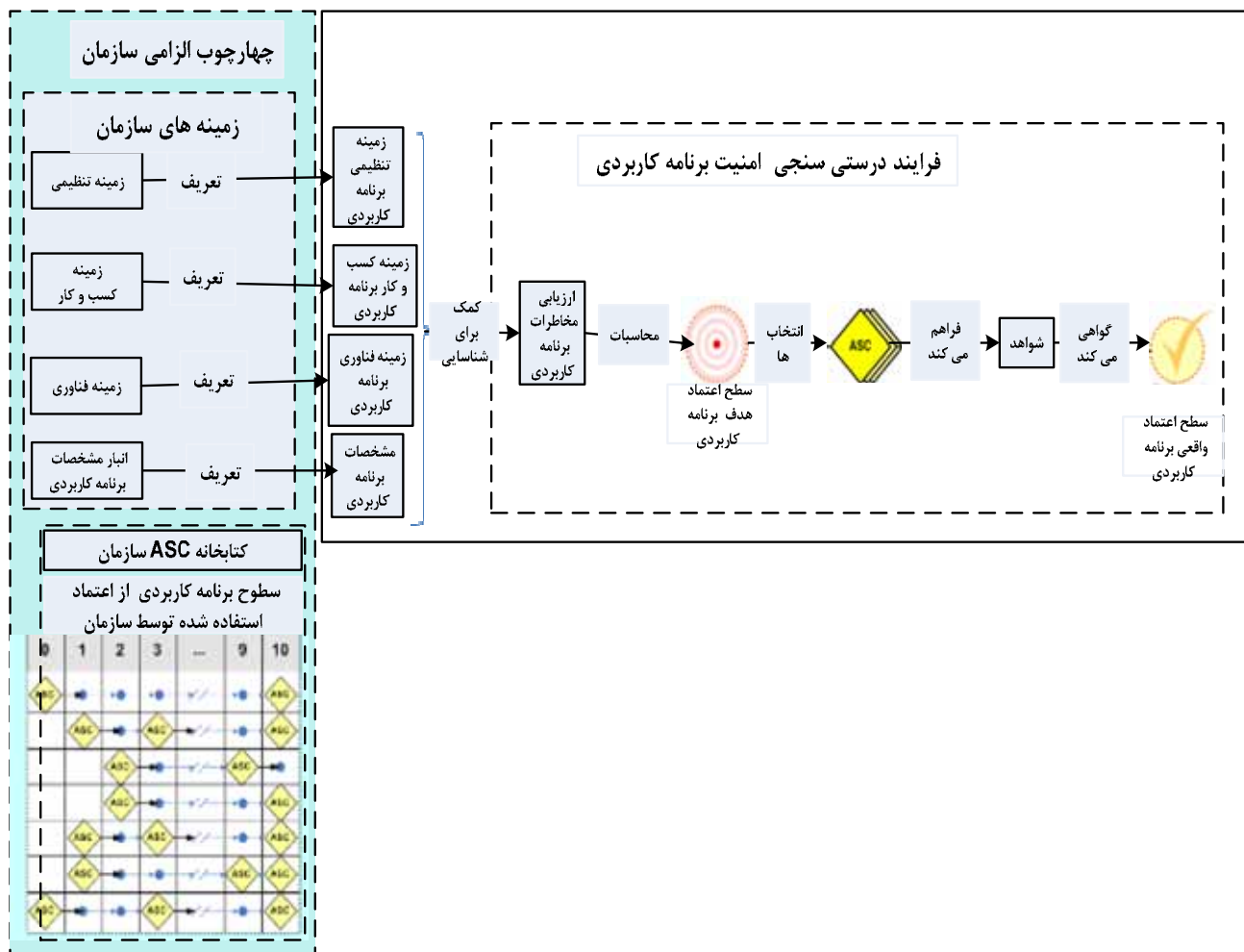
**مثال ۱-** سازمان باید این مرحله را به شکل دوره‌ای برای نظارت بر وضعیت پیاده‌سازی شده امنیت در مرحله تحقق برنامه کاربردی اجرا کند.

**مثال ۲-** سازمان می‌تواند این مرحله را برای نمایش سطح اعتماد هدف‌گذاری شده برنامه کاربردی پیش از تأیید انتشار، اجرا کند.

**مثال ۳-** سازمان می‌تواند این مرحله را در جریان مراحل عملیاتی چرخه حیات برنامه کاربردی و به‌عنوان قسمتی از ممیزی امنیتی سالانه سازمان اجرا کند.

در این مرحله یک گروه درستی‌سنجی داخلی یا خارجی (بسته به سیاست‌های سازمانی موجود در ONF) اجرای تمام درستی‌سنجی‌های تعیین‌شده توسط کنترل امنیت برنامه را در چارچوب الزامی برنامه کاربردی و نتایج به‌دست آمده بررسی می‌کند. هدف این مرحله نمایش سطح اعتماد هدف‌گذاری شده برنامه کاربردی در مقطع زمانی خاص است. سازمان، زمانی می‌تواند برنامه کاربردی را امن معرفی کند که سطح اعتماد واقعی آن با سطح اعتماد هدف‌گذاری شده برابر شود.

این مرحله برابر با مرحله «پذیرش مخاطره» موجود در فرآیند مدیریت مخاطره ذکر شده در استاندارد ملی ۲۷۰۰۵ است.



شکل ۱۴: مروری بر فرایند درستی سنجی امنیت برنامه کاربردی

## ۸-۵-۲ مولفه ها

### ۸-۵-۲-۱ سطح اعتماد واقعی برنامه کاربردی

سطح اعتماد واقعی برنامه کاربردی بالاترین سطح اعتماد مشخص شده توسط گروه درستی سنجی براساس سنجش درستی سنجی تمام کنترل های امنیت های برنامه کاربردی است.

هر یک از کنترل های امنیت برنامه کاربردی موجود در چارچوب الزامی، شامل عملکرد درستی سنجی مفصلی است که باید توسط گروه درستی سنجی اجرا شود و مرحله مورد نظر در چرخه حیات برنامه کاربردی را برای اجرای این سنجش مشخص می کند.

سطح اعتماد واقعی برنامه کاربردی با سنجش کنترل امنیت برنامه کاربردی به دست می آید که کنترل امنیت برنامه کاربردی نیز باید به نوبه خود در مقطع خاصی از چرخه حیات برنامه کاربردی کامل شود. چنانچه کنترل امنیت برنامه کاربردی در درستی سنجی رد شود، سازمان باید اقدامات لازم برای تصحیح شرایط را فراهم آورد.

دستیابی موفق به سطح اعتماد هدفمند برنامه کاربردی زمانی تأیید می‌شود که شواهد، صحت فعالیت‌های درستی‌سنجی مورد نظر را برای تمامی کنترل امنیت برنامه کاربردی مورد انتظار تأیید کنند. بعد از این تأیید، برنامه کاربردی، توسط سازمان امن در نظر گرفته شده اند برای استفاده کاربر یا کارمند از زمان صدور این تأییدیه تا درستی‌سنجی دوره‌ای بعدی که توسط الزام بازنگری متناوب در ۵ مرحله ASMP یا دیگر الزامات سازمان اجباری می‌شود.



## پیوست الف

### (اطلاعاتی)

#### نگاشت فرایند توسعه موجود در مطالعه موردی استاندارد ملی ISO/IEC 27034

#### الف-۱ کلیات

هدف این پیوست، نشان دادن این است که چگونه فرایند توسعه نرم‌افزاری مبتنی بر امنیت واقعی با بسیاری از مولفه‌ها و فرایندهای این استاندارد ملی نگاشت پیدا می‌کند. مگر در مواردی که به‌طور خاص اشاره شد. این مطالعه موردی فرض می‌کند که تمام فعالیت‌ها و نتایج عملکرد باید مطابق با این استاندارد ملی باشد. این پیوست، مفاهیم زیر را در حمایت از این استاندارد ملی شرح خواهد داد.

الف) مروری کوتاه بر امنیت توسعه چرخه حیات

ب) نگاشت فعالیت‌های امنیت توسعه با چارچوب سازمان. به‌طور خاص این پیوست:

- ۱) توضیح راجع به اتصالات داخلی بین زمینه‌ای فنی، کسب و کار و مقررات تنظیم شده می‌دهد.
- ۲) فرایندهای ایجاد و حفظ مشخصات برنامه کاربردی‌ها را تشریح می‌کند.
- ۳) نقش‌ها و مسئولیت‌های افراد مختلف درگیر در برنامه کاربرد فرایند توسعه را ترسیم می‌کند.
- ۴) کاربرد کنترل‌های امنیتی در محل را نمایش می‌دهد.
- ۵) در مورد فرایند درستی سنجی امنیت برنامه کاربردی بحث می‌کند.
- ۶) ترسیمی دیداری از کاربرد امنیتی مدل مرجع چرخه حیات فراهم می‌کند.
- ۷) مثال‌هایی از مازاد فعالیت‌های یک سازمانی که از فرایند کاربردی توسعه باید برای انجام فعالیت‌های مطابق با این استاندارد ملی استفاده می‌کند را فراهم سازد.

برای سهولت بررسی، شرح کلمه به کلمه و جزئی از کنترل در این بخش طبق این استاندارد ملی در شکل زیر برای هر قسمت اشاره شده است. سپس هر یک از آنها با یک مثال از کاربرد آن دنبال می‌شود. در جاهایی که ممکن است، ارجاع به منابع عمومی اطلاعات ارائه شده است. لینک وب‌ها برای توصیف ویژه فرایندها، ابزارها و اطلاعات جانبی دیگر می‌تواند به‌وسیله این استاندارد ارائه شود.

مهم است توجه داشته باشید که نویسندگان این پیوست، صرفاً بر نرم‌افزار امنیتی روش توسعه که در انتقال برنامه‌های کاربردی نرم‌افزارهای تجاری و سرویس‌های آنلاین استفاده می‌شود تمرکز می‌کند. فرآیندهای دیگری وجود دارد که وظایف امنیتی فناوری اطلاعات را پوشش می‌دهد. گروه‌هایی که مدیریت این فرایندها را بر عهده دارند، محدود به فناوری‌ها و زمینه‌های نظارتی مشابهی هستند، اما نرم‌افزارهای کاربردی برای استفاده عمومی گسترده را در نظر نمی‌گیرند.

در حالیکه تشریح هر دوی فناوری اطلاعات و روش‌های توسعه نرم‌افزارهای امنیتی ممکن به‌طور جالبی به برخی افراد اثبات کند که این موارد لزوماً شواهد قانع‌کننده‌ای از به‌کارگیری این استاندارد فراهم

نمی‌کند. استفاده از چرخه توسعه امنیت در این زمینه، به‌وسیله سازمان بین‌المللی استانداردسازی (ISO) تأیید نمی‌شود.

## الف-۲ چرخه توسعه امنیت

چرخه توسعه امنیت، یک نرم‌افزار تضمین رویه امنیتی است. به‌عنوان یک ابتکار و یک سیاست اجباری از سال ۲۰۰۴، چرخه توسعه امنیت نقشی حیاتی در تعبیه امنیت و حریم خصوصی در نرم‌افزار و شرکت‌های پذیرفته شده ایفا کرده است. چرخه توسعه امنیت با ترکیبی از یک رویکرد جامع و علمی، وظیفه حفظ امنیت و حریم خصوصی را در تمام مراحل فرایند توسعه به عهده دارد. ارجاع به فناوری‌های اختصاصی و منابع از این پیوست حذف شده‌اند.

چرخه توسعه امنیت همان‌طور که در شکل الف-۱ نمایش داده شده، شامل ۷ مرحله است:



شکل الف-۱- چرخه توسعه امنیت

## الف-۳ تطابق چرخه توسعه امنیت با چارچوب الزامی سازمان

یک توضیح ساده از کاربرد توسعه امنیت با چارچوب الزامی سازمان شامل موارد زیر می‌شود. مطالب زیر در مورد چرخه توسعه امنیت تحت این فرمت است.



## کلید کلمات اختصاری

PG	Product Group	گروه محصولات
LCA	Legal and Corporate Affairs	امور حقوقی و قانونی
LOB App	line of business Application	اختصاص برنامه‌های کاربردی در حمایت از کسب‌وکار و زمینه‌های فناوری
SDL	Security Development Lifecycle	توسعه امنیت چرخه حیات
HR	Human Resources	منابع انسانی
FSR	Final Security Review	بررسی میزان ایمنی نهایی

## الف-۴ زمینه کسب و کار

زیربند ۸-۱-۲-۱ فهرست‌های زمینه کسب و کار و اسناد تمام استانداردها و بهترین شیوه اتخاذ شده توسط سازمان که می‌تواند پروژه‌های کاربردی را تحت تأثیر قرار دهد. زمینه کسب و کار شامل موارد زیر می‌شود:

(الف) مدیریت توسعه پروژه، تحلیل مخاطره، فرایندهای عملیاتی، ممیزی و کنترل فرایندها

(ب) سیاست امنیتی سازمان

(پ) شیوه نوین برای زمینه کسب و کار

(ت) توسعه روش‌های مورد استفاده توسط سازمان

(ث) بیان بهترین شیوه‌ها برای کاربردهای مورد استفاده توسط سازمان در زمینه فناوری

(ج) فرایند مدیریت پروژه‌ای رسمی سازمان

(چ) پذیرش سایر استانداردهای بین‌المللی مرتبط با استاندارد ملی ISO/IEC 27001 ، ISO/IEC 27002 و ISO/IEC 5288

زمینه کسب و کار به وسیله ترکیبی از سیاست‌های شرکت‌های بزرگ، سیاست‌های منطقه‌ای خاص، زمینه فنی و فناوری و حضور بازار در واحدهای کسب و کار فردی در شرکت تنظیم می‌شود.

امنیت در توسعه تولید نرم‌افزار برای شرکت‌های نسبتاً گسترده در زمینه چرخه توسعه امنیت، ایجاد التزام و تعهد می‌کند. این چرخه همچنین نیازمند به تعیین افراد، فرایندها و کنترل جهت پیگیری پیشرفت در زمینه امنیتی و دستیابی به اهداف حفظ حریم خصوصی است.

توجه به طیف گسترده‌ای از حالات استقرار و سامانه‌های توسعه و پایبندی اجباری به مجموعه‌ای ثابت از روش‌های توسعه یا ابزارها امکان‌پذیر نیست. بنابراین گروه‌های کسب و کار مجاز به مقابله با چالش‌های فنی هستند که مستقیماً توسط سیاست چرخه توسعه امنیت تحت پوشش قرار نمی‌گیرند. (که این موارد با جزئیات بیشتر در نقش‌ها، مسئولیت‌ها و بخش مدارک زیر مشخص شده است.)

## الف-۵ زمینه مقررات تنظیم شده

زیربند ۸-۱-۲-۲ موارد چارچوب نظارتی و اسناد مرتبط با قوانین یا مقررات در هر یک از مکان‌های کسب و کار یک سازمان، می‌تواند پروژه‌های کاربردی را تحت تأثیر قرار دهد که شامل قوانین و مقررات کشورها یا زمینه‌های قضایی، جایی که در آن موارد کاربردی گسترش و توسعه یافته‌اند یا مستقر شده‌اند یا مورد استفاده قرار می‌گیرد.

استقرار سازمان یا استفاده از کاربردهای مشابه در بیش از یک کشور، ممکن است نیازمندی‌های امنیتی متفاوتی برای هر کشور داشته باشد. پیروی از مقررات و تحلیل ژئوپلیتیکی توسط فرایندهای کسب و کار موجود پوشش داده می‌شود و فعالانه برای اطلاع‌رسانی به فعالیت‌های طراحی و توسعه تیم‌های پروژه مورد استفاده قرار می‌گیرد.

سیاست‌ها به وسیله واحدهای کسب و کار و امور حقوقی مورد تحلیل قرار می‌گیرند. برای اطمینان از اینکه تمام جنبه‌های ایجاد و انتشار برنامه‌های کاربردی با معیارهای شناخته شده حقوقی و قانونی در مناطق مختلف روبرو می‌شوند و هر پروژه جدید براساس چارچوب سیاست‌های موجود عمل می‌کند. برخی از برنامه‌های کاربردی (همراه با موارد ذکر شده در بالا)، به وسیله تیم‌های محصول استفاده می‌شوند که به طور خودکار فرایند تضمین تطابق مقررات را برای نرم‌افزارهای کاربردی و استفاده عمومی توسعه می‌دهند. در نهایت، خروجی بررسی‌های نظارتی با خروجی فرایندهای تأیید کاربردهای امنیتی (بحث شده در زیر) یک نمایش عینی و مفهومی از فرایند کاربرد توسعه امنیت ایجاد می‌کند. با این حال مهم است توجه کنیم که سیاست‌های نظارتی و ژئوپلیتیک به وسیله چرخه توسعه امنیت تعیین نمی‌شوند.

## الف-۶ انبار مشخصات برنامه کاربردی

زیربند ۸-۱-۲-۳ انبار مشخصات برنامه کاربردی، الزامات کارکردی کلی فناوری و راه حل‌های از پیش تأیید شده مطابق با آنها را فهرست و ثبت می‌کند. مشخصات برنامه باید شامل موارد زیر باشد:

الف) محاسبه ویژگی‌های کاربردی، ذخیره سازی و انتقال اطلاعات

ب) پارامترهای معمول، برنامه، ویژگی‌ها، خدمات و الزامات

پ) کد منبع، کد باینری، محصولات یا خدمات استفاده شده یا متکی به برنامه‌های کاربردی

سایر مشخصات که ممکن است شامل جزئیات چگونگی تعامل با برنامه‌های کاربردی باشند، عبارتند از:

الف) سامانه‌های دیگر

ب) زمان اجزای زیرساخت‌ها که بستگی به عوامل متعددی دارد.

پ) فهرست کنترل در محیط و زمان اجرا

مشخصات نوشته و به وسیله واحدهای کسب و کار فردی ذخیره می‌شوند و به طور کلی شامل دو عملکرد می‌شوند: تعیین اینکه چگونه یک جزء خاص باید محاسبه، ذخیره و اطلاعاتش انتقال یابد و راهنمایی فنی (تعیین زبان‌های برنامه‌نویسی، مترجم‌ها و...)

در برخی موارد، چرخه توسعه امنیت، سیاست‌هایی را برای اجزا یا فناوری‌های دیگر که دارای زمینه امنیتی هستند (برای مثال کتابخانه‌هایی برای ارائه خدمات رمزنگاشتی)، برای اطمینان از امنیت برنامه‌های کاربردی و حریم خصوصی توسط الزامات کارکردی یا تسهیلات نباید در معرض خطر قرار گیرد.

## الف-۷ زمینه فناوری

**۸-۲-۱-۴** زمینه فناوری شامل موجودی تمام محصولات، خدمات و فناوری‌های در دسترس سازمان برای پروژه‌های برنامه کاربردی است. این محصولات، خدمات و فناوری‌ها تهدیدی که برنامه‌های کاربردی در معرض آن هستند را تعیین می‌کنند. زمینه فناوری شامل رایانه‌ها، ابزار، محصولات فناوری اطلاعات، خدمات، زیرساخت‌های ارتباطی و سایر دستگاه‌های فنی است.

**مثال** - زمینه‌های فناوری که ممکن است تاثیر بر امنیت برنامه کاربردی که شامل زیرساخت کارخواه - کارساز، زیرساخت وب، زیرساخت شبکه و محیط توسعه و ابزار داشته باشد.

زمینه فناوری اغلب در سراسر واحدهای کسب و کار متفاوت است و از ترکیبی از مشتقات بازار در صورت هماهنگی و سازگاری و استانداردهای فنی برای یک گروه خاص حاصل می‌شود.

با توجه به تنوع در استانداردها برای محصولات فناوری اطلاعات، خدمات و فناوری در سراسر واحدهای کسب و کار و زمینه فناوری که به‌طور مستقل به‌وسیله هر واحد تجاری تنظیم می‌شود، به آنها اجازه رفع نیازهای خود را می‌دهد. با این حال واحدهای کسب و کار همچنین باید اطمینان دهند که پروژه‌های نرم‌افزاری از خدمات فناوری اطلاعات استفاده می‌کنند و فناوری به آنها اجازه می‌دهد معیارهای امنیتی داشته باشند که در زمینه کسب و کار و نظارت تنظیم می‌شوند.

## الف-۸ نقش‌ها، مسئولیت‌ها و صلاحیت‌ها

**۸-۲-۱-۵** ONF باید شامل موارد زیر شود:

الف) فهرست و شرح همه نقش‌ها، مسئولیت‌ها و صلاحیت‌های حرفه‌ای مورد نیاز برای افراد درگیر در ایجاد و حفظ چارچوب و نقش‌های مختلف برای ایجاد و حفظ کاربرد کنترل‌های امنیتی

ب) فهرست و شرح همه نقش‌ها، مسئولیت‌ها و صلاحیت‌های حرفه‌ای مورد نیاز برای افراد درگیر در برنامه کاربردی سازمان مثل مدیریت امنیت اطلاعات، مدیران پروژه، مدیران سرپرست، تحصیل نرم‌افزار، مدیران توسعه نرم‌افزار، صاحبان برنامه‌های کاربردی، مدیران کاربر، معماران، برنامه نویسان، آزمایش‌کنندگان، مدیران سامانه، پایگاه داده مدیران، مدیران شبکه و کارکنان فنی.

این یک سیاست گسترده سازمانی است که اطمینان می‌دهد تمام نقش‌های حیاتی برای تمام مراحل مشخص شده‌اند، تمام مسئولیت‌ها تعریف شده‌اند که از تضاد منافع اجتناب شود و افرادی که این نقش‌ها را به عهده می‌گیرند، دارای مدارک حرفه‌ای کافی هستند.

طبقه‌بندی شغلی و کارکنان توسط بخش منابع انسانی با ورود واحدهای کسب و کار ایجاد و نگهداری می‌شوند. این گروه‌ها شامل توصیف سطوح بالای وظایف و صلاحیت‌های منحصربه‌فرد برای هر نقش شغلی هستند. در حالی که منابع انسانی شرح برخی از مشاغل را حفظ می‌کنند ولی عموماً واحدهای کسب و کار در مورد چگونگی تعیین طبقه‌بندی مشاغل به‌طور خاص با توجه به صلاحیت‌های امنیتی یا مسائل خصوصی، تصمیم می‌گیرند و به‌کارگیری مجموعه‌ای از این معیارها کمک به مسئولیت امنیت جهت نظارت در یک تیم توسعه خواهد بود.

فرایند توسعه نرم‌افزار، دارای معیارهای عمومی و شرح کار برای نقش‌های امنیتی و خصوصی است، این نقش‌ها در طی مراحل مورد نیاز برای فرایند توسعه نرم‌افزار اختصاص داده می‌شوند. نقش‌های ویژه شغلی باید قبل از شروع مرحله توسعه تعریف شوند. این نقش‌ها طبیعتاً مشورتی بوده و یک چارچوب لازم جهت شناسایی، کاهش امنیت را فراهم کرده و مسائل مربوط به حریم خصوصی در پروژه‌های توسعه نرم‌افزار ارائه می‌شوند. این نقش‌ها عبارتند از:

**نقش‌های نظارتی:** این نقش‌ها جهت ارائه نظارت بر پروژه طراحی شدند و ممکن است شامل مشاوره کمی و کیفی به تیم‌های پروژه جهت ایجاد یک حداقل اطمینان قابل قبول و ایجاد آستانه اطمینان برای یک پروژه کاربردی باشند. نقش‌های نظارتی باید به مقامات ذی‌صلاح جهت پذیرش یا رد امنیت و حفظ حریم خصوصی برنامه‌ها واگذار شوند. در یک پروژه تیمی:

**الف) مشاور امنیتی:** این نقش توسط افرادی با تخصص امنیت فردی از بیرون از افراد تیم پروژه ایجاد می‌شود. این نقش همچنین می‌تواند توسط یک گروه زبده مستقل که تمرکز بر امنیت گروهی و جمعی سازمان دارند، با دنبال کردن خدمات کارشناسان خارجی به سازمان ارائه شود. شخص انتخاب‌شده برای این وظیفه باید دو نقش فرعی زیر را ایفا کند:

**۱) ممیز:** این فرد باید بر هر مرحله از فرایند توسعه امنیت نظارت کند و بر پایان موفقیت‌آمیز الزامات هر مرحله گواهی کند. مشاور امنیتی باید آزادی کافی جهت گواهی دادن بر انطباق (یا عدم انطباق) با الزامات امنیتی بدون دخالت تیم پروژه را داشته باشد.

**۲) کارشناس:** فرد انتخاب‌شده برای نقش مشاور امنیتی باید موضوعات قابل تأییدی با تخصص در امنیت در اختیار بگذارد.

**ب) مشاور در زمینه مسائل خصوصی:** این نقش توسط کارشناس مسائل خصوصی و فردی از بیرون از تیم پروژه انتخاب می‌شود. این نقش همچنین می‌تواند توسط یک عضو خبره واجد شرایط مستقل درون سازمان که بر مسائل خصوصی گروه تمرکز می‌کند، یا با جستجوی خدمات از کارشناسان خارجی بیرون از سازمان تعیین شود. فردی که این زمینه شغلی را دربر می‌گیرد باید دو نقش فرعی زیر را ایفا کند:

**۱) ممیز:** این فرد باید بر رویه توسعه حریم خصوصی نظارت کند و بر پایان موفقیت‌آمیز هر مرحله مورد نیاز گواهی دهد. مشاور در این زمینه باید آگاهی کافی جهت گواهی دادن بر انطباق یا عدم انطباق با الزامات خصوصی بدون وجود دخالتی از تیم‌های پروژه داشته باشد.

**۲) کارشناس:** فرد انتخاب شده برای نقش مشاور در زمینه حریم خصوصی باید تخصص قابل تأیید در این زمینه را داشته باشد.

ترکیبی از نقش‌های مشورتی: نقش مشاور امنیتی ممکن است با نقش مشاور حریم خصوصی ترکیب شود. فرض کنید که یک فرد با مهارت و تجربه مناسب را می‌توان شناسایی کرد.

**نقش‌های اصلی تیم:** نقش‌های اصلی تیم باید توسط کارشناسانی اتخاذ شود که پروژه تیم‌های توسعه را در بحث و مذاکره با مشاوران امنیت و حفظ حریم خصوصی ارائه می‌کنند. این نقش مسئول مذاکره، پذیرش و ردیابی حداقل نیازهای امنیتی، حفظ خطوط روشنی از ارتباط با مشاوران و سایر تصمیم‌گیرندگان در طول مدت پروژه توسعه نرم‌افزار است.

**الف) راهنمای تیم امنیت:** این فرد (یا گروهی از افراد)، مسئولیتی از این جهت که تضمین کند انتشار نرم‌افزار، تعیین‌کننده تمام موضوعات امنیتی است را ندارند. با این حال، این فرد مسئول هماهنگی و پیگیری مسائل امنیتی پروژه است. این فرد همچنین مسئول گزارش وضعیت به مشاور امنیتی و سایر افراد مربوط (برای مثال راهنمای توسعه و ...) در تیم پروژه است.

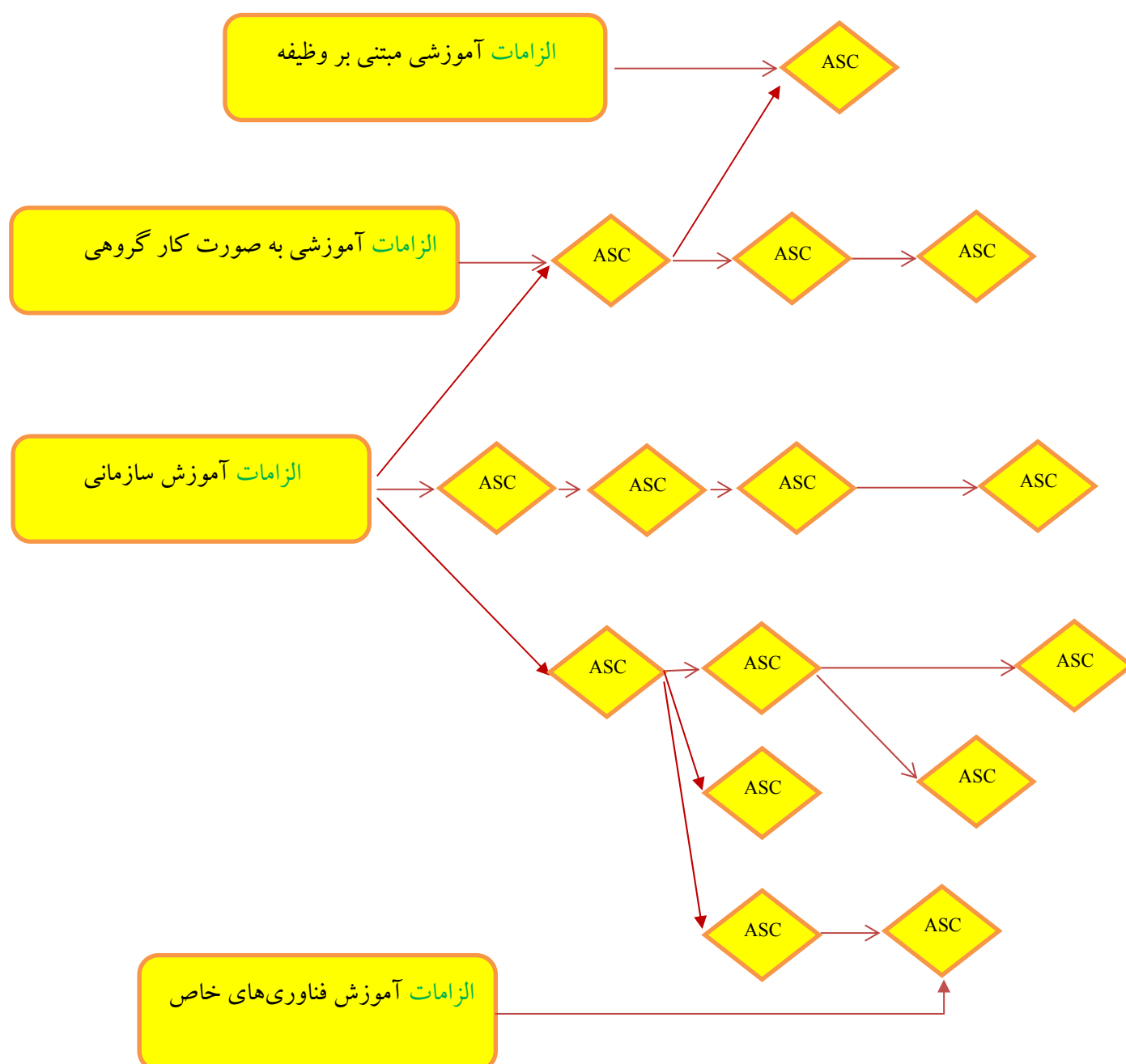
**ب) راهنمای تیم حریم خصوصی:** این فرد (یا گروهی از افراد)، مسئولیتی از این جهت که تضمین کند انتشار نرم‌افزار، تعیین‌کننده تمام موضوعات حریم خصوصی است را ندارد. با این حال، این فرد مسئول هماهنگی و پیگیری مسائل امنیتی برای پروژه است. این نقش همچنین مسئول گزارش وضعیت به مشاوران مسائل حریم خصوصی و سایر بخش‌های مرتبط (به‌عنوان مثال راهنمای توسعه و ...) در تیم پروژه است.

#### الف-۹ کتابخانه ASC سازمان

**۸-۲-۶** سازمان باید حداقل یک کتابخانه کنترلی برای کاربردهای امنیتی داشته باشد. این کتابخانه، کتابخانه کاربرد کنترل امنیتی نامیده می‌شود که فهرست و اسناد آن تماماً باید توسط سازمان به رسمیت شناخته شود. کتابخانه کاربردی کنترل امنیتی، از استانداردها، بهترین نقش‌ها و شیوه‌ها، مسئولیت‌ها و مدارک حرفه‌ای، فناوری، کسب و کار و زمینه‌های نظارتی و مشخصات کاربردی تکامل یافته است.

هفده بخش کاربردی کنترل امنیتی، به‌عنوان بخشی از فرایند توسعه نرم‌افزار که در زیر توصیف شده ، شناسایی شده‌اند. این مثال شامل هر دو وظایف اجباری و اختیاری می‌شود. آن بخش از وظایف کاربرد کنترل امنیتی که الزامی نیستند، ممکن است در صورت لزوم توسط واحدهای کسب و کار در راستای رسیدن به اهداف مطلوب امنیتی و اهداف حریم خصوصی، توسعه یابند. کتابخانه کاربردی کنترل امنیتی که در زیر ترسیم می‌شود از روش‌های سنتی توسعه استفاده می‌کند. به خاطر حفظ ایجاز و ارائه مفید مطالب بخش‌های مازاد تحت کاربرد کنترل امنیتی حذف شده است.

سمت چپ در کاربرد کنترل امنیتی زیر، به عنوان ASC «ریشه» در نظر گرفته می شود که در واقع «نقطه والد» از درخت ASC است که با جزئیات در شکل زیر نشان داده شده است. این شکل فرضی نشان می دهد که ASC به وسیله سازمانی با سطوح فزاینده پیچیدگی و جزئیات به کار می رود تا به حد اعتماد مورد نظر برای کاربردی که سازمان پیش از آغاز پروژه تعیین کرده بود برسد.



شکل الف-۳- مثالی از یک درخت ASC



## الف-۹-۱ آموزش

۱- الزامات آموزش: همه اعضای تیم توسعه نرم‌افزاری باید آموزش مناسب یافته تا آگاهی کافی درباره اصول امنیتی و رویه‌های اخیر در امنیت و حریم خصوصی را داشته باشند. افراد در نقش‌های شغلی فنی (توسعه‌دهندگان، آزمایش‌کنندگان و مدیران برنامه) که به‌طور مستقیم با توسعه برنامه نرم‌افزاری درگیر هستند، باید حداقل در یک کلاس آموزشی امنیتی در هر سال شرکت کنند. آموزش اساسی نرم‌افزار امنیتی، مفاهیم بنیادی مانند طراحی ایمن، مدل‌سازی تهدید، سنجش میزان سطوح نااطمینانی، برنامه‌نویسی ایمن، آزمون امنیتی و مسائل خصوصی.

## الف-۹-۲ الزامات

۲- الزامات امنیتی: نیاز به در نظر گرفتن امنیت و حریم خصوصی در یک سطح بنیادی، به‌عنوان یک جنبه اساسی از توسعه سامانه مطرح است. نقطه بهینه برای تحقق بخشیدن به الزامات یک برنامه کاربردی در طی مراحل برنامه‌ریزی اولیه یک مسئله جدید و مهم است. این به تیم‌های توسعه اجازه می‌دهد به‌منظور شناسایی نقاط عطف کلیدی و اجازه ادغام امنیت و حفظ حریم خصوصی در یک مسیری که هر اختلالی در طرح و برنامه را به حداقل برساند.

تحلیل الزامات امنیتی و حریم خصوصی در آغاز به کار هر پروژه و شامل اقدامات اجباری متفاوت از جمله: تعیین موارد کاربردی فرایند توسعه نرم‌افزار، تعیین افراد مسئول امنیت و نظارت بر حفظ حریم خصوصی است. (توجه به زیربند ۸-۱-۲-۵، نقش‌ها، مسئولیت‌ها و صلاحیت‌ها) و تعیین ویژگی‌های حداقل نیازهای امنیتی و مشخصات و شناسایی آسیب‌پذیری‌ها و عملیاتی که سامانه آن را پیگیری می‌کند.

۳- دروازه‌های کیفیت/نوارهای اشکال<sup>۱</sup>: دروازه‌های کیفیت و نوارهای اشکال برای ایجاد کمینه یک سطح قابل قبولی از کیفیت در امنیت و حفظ حریم خصوصی استفاده می‌شوند. تعیین این معیارها شروع انجام یک پروژه را بهبود می‌بخشد و درک صحیحی از مخاطرات مرتبط با موضوعات امنیتی را ایجاد می‌کند و تیم‌ها را قادر می‌سازد امنیت و نقصان‌های آن را در طی مسیر توسعه، شناسایی و تصحیح کنند. یک پروژه تیمی باید مذاکراتی در مورد میزان کیفیت در هر مرحله توسعه انجام دهد و این موارد نیز توسط مشاوران امنیتی در صورت لزوم با توضیحات خاص پروژه‌ای و الزامات امنیتی شدیدی پذیرفته می‌شود. همچنین تیم پروژه باید انطباق با مذاکراتی که در محدوده کیفیت انجام شد و در جهت تطابق با الزامات تأییدشده در بررسی‌های امنیتی بود را به عمل آورد. نوار اشکال محدوده‌ای از کیفیت تلقی می‌شود که شامل تمامی پروژه‌های توسعه نرم‌افزار است و جهت تعریف میزان محدودیت‌ها برای نقصان‌های امنیتی استفاده می‌شود و هرگز بدون فعالیت نیست، حتی زمانی که به تاریخ اتمام پروژه نزدیک هستیم.

۴- ارزیابی میزان مخاطره امنیت و حریم خصوصی: ارزیابی مخاطره امنیت و حریم خصوصی، فرایندهای الزامی برای شناسایی جنبه‌های کاربردی نرم‌افزار هستند که ممکن است نیاز به بررسی عمیق داشته باشد. با توجه به ویژگی‌های برنامه و قابلیت‌های عملی در نظر گرفته‌شده، بررسی از یک پروژه به پروژه

دیگر متفاوت است. منطقی است که ابتدا به ارزیابی ساده مخاطره اقدام و در صورت لزوم محدوده پروژه را گسترش و توسعه دهیم. چنین ارزیابی‌هایی باید شامل اطلاعات زیر باشد:

- الف) (امنیت) کدام بخش از پروژه به مدل‌های بررسی تهدیدات قبل از انجام آن، نیاز خواهد داشت؟  
ب) (امنیت) کدام بخش از پروژه نیاز به طراحی امنیتی قبل از انجام خواهد داشت؟  
پ) (زمینه امنیت) کدام بخش از پروژه (در صورت وجود) نیاز به آزمون با توافق گروهی که خارج از تیم مورد نظر ما هستند، دارد؟ هر بخش پروژه که نیاز به تست دارد باید مسائل شناسایی شده توسط اعضای این گروه را قبل از اینکه پروژه جهت انتشار آماده تصویب شود، حل کند.  
ت) (امنیت) هر تست دیگر یا تحلیل الزامات امنیتی توسط مشاور امنیتی که جهت کاهش مخاطره امنیتی لازم است، باید انجام شود.

ث) (امنیت) تعیین محدوده خاص مورد نیاز از تست fuzz (در قسمت ASC/12 در زیر)

ج) (حریم خصوصی) تعیین و رتبه‌بندی اثرات حریم خصوصی و موارد مرتبط به آن.

۱) P1: مخاطره بالای حریم خصوصی: ویژگی، محصول یا عرضه خدمات یا انتقال اطلاعات مشخص شناسایی، تنظیمات یا نوع فایل انجمن‌ها یا نصب نرم‌افزارها را تغییر می‌دهد.

۲) P2: مخاطره متوسط حریم خصوصی: تنها رفتاری که در ویژگی‌های حریم خصوصی یا بر محصولات و خدمات تأثیر می‌گذارد، انتقال داده‌های ناشناس توسط کاربر است. (به عنوان مثال کاربر بر روی یک لینک خاص کلیک می‌کند و به یک وب سایت می‌رود).

۳) P3: مخاطره پایین حریم خصوصی: هیچ رفتاری در ویژگی، محصول یا خدمات وجود ندارد که بر حریم شخصی و خصوصی تأثیر بگذارد. هیچ اطلاعات شخصی یا ناشناسی انتقال نمی‌یابد. هیچ اطلاعات شخصی یا شناسایی شده‌ای در ماشین ذخیره نمی‌گردد. هیچ تنظیماتی در طرف کاربر تغییر نمی‌کند و هیچ نرم‌افزاری نصب نمی‌شود.

## الف-۹-۳ طراحی

**۵- الزامات طراحی:** زمان بهینه برای تأثیرگذاری در طراحی قابل اعتماد برای یک پروژه در چرخه عمر آن است. این بسیار مهم است که نگرانی‌های امنیتی و حریم خصوصی به دقت در مراحل طراحی در نظر گرفته شود. کاهش میزان امنیت و موضوعات حریم خصوصی، زمانی که در مراحل ابتدایی چرخه پروژه انجام می‌شود، ارزش کمتری دارد. تیم‌های پروژه باید از یک سری عملیات خاص در مورد مسائل امنیتی و حریم خصوصی در نزدیک شدن به پایان مراحل توسعه پروژه خودداری کنند. علاوه بر این بسیار برای تیم پروژه مهم است که تمایز بین امنیت ویژگی‌ها یا ویژگی‌های امنیتی را درک کنند. ادراک این مفاهیم، پیاده‌سازی امنیت ویژگی‌ها که در واقع غیرمطمئن هستند را امکان‌پذیر می‌سازد.

ویژگی‌های امنیتی این گونه تعریف می‌شوند: ویژگی‌هایی که از نظر عملکردی با توجه به مسائل امنیتی به خوبی طراحی شده‌اند و شامل اعتبارسنجی دقیق تمام داده‌ها قبل از پردازش یا پیاده‌سازی قوی در مورد مطالعات کتابخانه‌ای برای خدمات رمزنگاشتی هستند. ویژگی‌های امنیتی، عملکرد برنامه‌ها را با توجه به مفاهیم امنیتی شرح می‌دهند (برای مثال احراز هویت Kerberos).

مشخصات طراحی نیاز به توصیف ویژگی‌های امنیتی یا ویژگی‌های حفظ حریم خصوصی دارد که به‌طور مستقیم به کاربران القا خواهد شد. از قبیل نیاز به احراز هویت کاربران برای دسترسی به اطلاعات خاص یا جلب رضایت کاربر قبل از استفاده از اطلاعاتی با مخاطره بالای حریم خصوصی. در نتیجه، تمام مشخصات طرح مورد نظر باید:

الف) با دقت و به‌طور کامل باید چگونگی اجرای این ویژگی‌ها را توصیف کند.

ب) چگونگی پیاده‌سازی ایمن تمام قابلیت‌ها توسط یکی از ویژگی‌های مورد نظر توصیف کند

پ) چگونگی استقرار ویژگی‌ها در یک مدل ایمن توصیف کند

الزامات طراحی شامل تعدادی از اقدامات مورد نیاز است که شامل اما محدود به بررسی طرح امنیت، حریم خصوصی، مشخصات آن و پیاده‌سازی حداقل رمزنگاشتی مورد نیاز طراحی است.

۶- کاهش سطحی حمله: کاهش سطحی حمله با مدل‌سازی آن در تراز وسط قرار می‌گیرد، اگرچه موضوعات امنیتی از جنبه‌های نسبتاً متفاوتی بررسی می‌کند. کاهش سطحی حمله، ابزاری است جهت کاهش مخاطره؛ به این طریق که به موارد مخاطره، جهت پیدا کردن یک نقطه ضعف یا آسیب‌پذیری احتمال و شانس کمتری می‌دهد.

کاهش سطحی حمله به وسیله کاهش دادن، متوقف کردن یا محدود کردن دسترسی به خدمات سامانه و پذیرش اصل حداقل دسترسی به مکان‌های ممکن، تحقق می‌یابد.

۷- مدل‌سازی تهدید: مدل‌سازی تهدید، یک فرایند الزامی انجام‌شده در مرحله طراحی است که به تیم‌های توسعه اجازه می‌دهد تا در نظر بگیرند، مکتوب کنند یا در مورد مفاهیم امنیتی طرح به شکل ساختاری بحث کنند. این مدل‌سازی همچنین اجازه توجه الزامی به مسائل امنیتی را به‌صورت جزئی یا در سطح کاربردی می‌دهد. مدل‌سازی تهدید، یک فعالیت تیمی است که شامل اجزایی چون مدیران برنامه‌ها/پروژه، برنامه‌ریزان، توسعه‌دهندگان و... می‌شود و یک تحلیل اساسی امنیتی را مبتنی بر وظیفه در طول مراحل طراحی نرم‌افزار ارائه می‌کند.

#### الف-۹-۴ پیاده‌سازی

۸- استفاده از ابزارهای مصوب: تمامی تیم‌های توسعه باید فهرستی از ابزارهای تأییدشده (قابلیت‌های امنیتی خاص مانند مترجم‌ها و ...) را برای استفاده در برنامه‌های نرم‌افزاری تعریف کرده و انتشار دهند. این فهرست باید توسط مشاور امنیتی برای اعضای تیم پروژه شناسایی و تأیید می‌شود. به‌طور کلی، تیم‌های توسعه باید تلاش کنند جهت استفاده از آخرین نسخه ابزارهای مصوب از قابلیت‌های امنیتی جدید منتفع شوند.

۹- عدم رضایت از عملکردهای بدون امنیت: بسیاری از عملکردهای مورد استفاده و رایج و برنامه‌های کاربردی، در مواجهه با تیم‌های پروژه تهدیدات زیست‌محیطی ایمن نیستند و باید تحلیل شوند. تمام عملکردها و برنامه‌های کاربردی که در ارتباط با پروژه توسعه نرم‌افزار مورد استفاده قرار خواهد گرفت و مانع از آن شود که امنیت کافی را نداشته باشد.

پس از آنکه این فهرست تهیه شد، تیم‌های پروژه باید از فایل‌ها، مترجم‌های جدیدتر یا ابزارهای اسکن کد مخصوص چک کردن آن، برای اعتماد از عدم استفاده از برنامه‌های عملکردی محدودشده و جایگزینی آن با موارد دارای امنیت بیشتر استفاده کنند.

**۱۰- تحلیل ایستا:** تیم پروژه باید تحلیل کد پایدار از انواع کد را انجام دهند. تحلیل پایدار از انواع کد یک راه حل قیاس‌پذیر برای بررسی کد امنیتی فراهم می‌کند و می‌تواند مورد استفاده قرار گیرد و اعتماد دهد که منجر به سیاست‌های کدگذاری امنیتی تنظیم‌شده توسط تیم امنیتی می‌شود و پیش‌روی مشاور امنیتی قرار می‌گیرد.

تحلیل کد پایدار به خودی خود، عموماً ناکافی است. برای انجام بررسی‌های امنیتی کامل، تیم امنیتی و مشاوران امنیتی باید از نقاط ضعف و قوت ابزارهای تحلیل پایدار آگاه بوده و آماده ارائه کد بررسی وظایف با سایر ابزارها و بررسی منابع انسانی به‌طور مناسبی باشند. تحلیل سطحی ایستا در مورد چرخه توسعه نرم‌افزار در چک کردن به موقع کد، با استفاده از تحلیل عملکرد رخ می‌دهد. سایر کارکردهای تحلیل پایدار در مواقع لزوم انجام می‌گیرد.

#### الف-۹-۵ تایید

**۱۱- تحلیل برنامه پویا:** تأیید زمان اجرای برنامه‌های نرم‌افزاری ضرورت دارد تا اطمینان حاصل شود که قابلیت یک برنامه نرم‌افزاری مانند آنچه طرح‌ریزی شده هست. این تأیید عملکردی باید ابزارهایی را که بر رفتار عملکردی نظارت می‌کند، از جهت نداشتن ضعف، استفاده از امتیاز مسائل یا سایر موضوعات انتقادی امنیتی، مشخص کند. فرایند توسعه نرم‌افزار از ابزارهای مبتنی بر زمان اجرا به همراه سایر فناوری‌ها مانند تست fuzz برای دست‌یافتن به سطوح مطلوب پوشش تست امنیتی استفاده می‌کند.

**۱۲- تست fuzz:** این تست جهت رفع مشکلات برنامه به‌وسیله شناسایی نقص برنامه‌ها یا بررسی استفاده از داده‌های تصادفی به‌عنوان ورودی برنامه‌ها استفاده می‌شود. چرخه توسعه، نرم‌افزار تست fuzz انجام‌شده بر روی برنامه‌های متعدد و موارد مشابه آن را مشخص می‌کند. این تست از نظر عملکردی در برنامه‌های کاربردی مورد نظر و مشخصات مورد توجه عملکردی و فنی برای نرم‌افزارهای کاربردی استفاده می‌شود. مشاور امنیتی ممکن است نیاز به تست‌های fuzz بیشتر یا افزایش دامنه و مدت این تست را براساس عملکرد برنامه کاربردی مورد نظر لازم بداند.

**۱۳- بررسی مدل تهدید/ تهدید سطحی:** این بررسی برای یک برنامه کاربردی که انحراف قابل توجهی از مشخصات عملکردی و فنی ایجادشده در طول مسیر طراحی یک پروژه توسعه نرم‌افزار دارد، رایج است. بنابراین بررسی مدل‌های تهدید و اندازه‌گیری تهدیدات سطحی یک برنامه کاربردی ارائه‌شده، زمانی که کد آن در حال تکمیل است؛ بسیار مهم است. این بررسی اطمینان می‌دهد که هر تغییری در سامانه در نظر گرفته شده و تعدیل می‌شود.

**۱۴- بررسی کد راهنما (اختیاری):** بررسی کد راهنما به‌عنوان یک وظیفه اختیاری در چرخه توسعه نرم‌افزاری تلقی می‌شود. بررسی این کد، معمولاً توسط اعضای تیم امنیت کاربردی با توجه به توصیه مشاوران امنیتی انجام می‌شود. در حالی که ابزارهای تحلیل می‌توانند کار شناسایی ضعف‌ها یا آسیب‌پذیری‌ها

را انجام دهند، اما کامل نیستند. بررسی کد راهنما معمولاً بر اجزای بحرانی یک کاربرد تمرکز می‌کند و اغلب در جایی که داده‌های حساس مانند اطلاعات شناسایی شخص درگیر می‌شوند، مورد استفاده قرار می‌گیرد. این راهنما همچنین در بررسی‌های سایر اجزای حساس استفاده می‌شود.

#### الف-۹-۶ انتشار

**۱۵- طرح پاسخ به پیشامد:** موضوع گشایش و انتشار هر نرم‌افزاری که از الزامات چرخه توسعه نرم‌افزاری است، باید شامل یک طرح واکنش به مسائل باشد. هر برنامه‌ای حتی بدون آسیب‌پذیری‌های شناخته شده در زمان گشایش، می‌تواند موضوع تهدیداتی باشد که با گذشت زمان پدیدار می‌شود. طرح واکنش به مسائل شامل موارد زیر است:

الف) یک تیم شناسایی، حتی اگر کوچک باشد، با توجه به منابع خود باید دارای یک طرح واکنش در مواقع اضطراری باشد که این طرح مشخص می‌کند ۳ تا ۵ نفر از کارکنان مهندسی، ۳ تا ۵ نفر بازاریاب و ارتباط با مشتری و حداقل ۲ نفر در بخش مدیریت کارکنان که به‌عنوان یک نقطه شروع بتواند در مواقع اضطراری ایجاد امنیت کنند.

ب) ۳۶۵X۷X۲۴ ارتباط تلفنی با فرد تصمیم‌گیرنده

پ) طرح خدمات امنیتی برای کدهای به‌جا مانده سایر گروه‌ها در سازمان

ت) طرح امنیت خدماتی برای مجوز و کد طرف سوم، این طرح شامل نام فایل، نسخه‌ها، منبع کد، اطلاعات تماس طرف سوم و مجوز قراردادی برای ایجاد تغییرات (اگر مناسب باشد)

**۱۶- بازنگری امنیتی نهایی:** این بازنگری شامل بررسی دقیق از تمام فعالیت‌های امنیتی انجام‌شده، براساس برنامه‌های کاربردی نرم‌افزار، قبل از انتشار آن است. این بررسی توسط مشاور امنیتی با کمک کارکنان منظم بخش توسعه و هدایت تیم امنیتی و حفظ حریم خصوصی انجام می‌شود. این بررسی یک بررسی ساده نیست، در واقع فرصتی برای انجام فعالیت‌های امنیتی است که قبلاً نادیده گرفته شده یا فراموش شده‌اند. این بررسی معمولاً شامل بررسی مدل‌های تهدیدکننده، بررسی درخواست‌های خاص مورد انتظار، بررسی ابزار و عملکرد از نظر کیفیت مشخص‌شده قبلی است. این بررسی، سه نتیجه خواهد داشت:

الف) **بررسی نهایی امنیتی گذشته:** تمام موضوعات امنیتی و حفظ حریم خصوصی که توسط فرایند بررسی نهایی شناسایی می‌شوند، ثابت هستند یا کاهش می‌یابند.

ب) **بررسی نهایی امنیتی گذشته با استثناء:** تمام موضوعات امنیتی و حریم خصوصی که توسط این فرایند بررسی می‌شوند، ثابت هستند و بررسی‌هایی که نمی‌توانند به درستی تعیین شوند، اصلاح شده و در نسخه تصحیح شده بعدی وارد سامانه می‌شوند.

پ) **بررسی نهایی امنیتی به صورت مداوم:** اگر یک تیم با تمام الزامات چرخه توسعه نرم‌افزار مواجه نباشند و مشاور امنیتی و تیم تولید نتوانند به مصالح قابل قبول دسترسی یابند، مشاور امنیتی نمی‌تواند پروژه را تأیید کند و این پروژه نمی‌تواند انتشار یابد. تیم‌ها باید کلیه الزامات چرخه توسعه نرم‌افزار را

تعیین کنند مبنی بر این که می‌توانند آن را راه‌اندازی کرده یا مدیران اجرایی را مجبور به تصمیم‌گیری در این زمینه کنند.

**یآوری - نتایج FSR** به مفهوم سطح واقعی اعتماد نزدیک است چنانچه FSR بررسی آزمون تمامی عملکرد فعالیت‌های امنیت بر روی نرم افزار برنامه کاربردی پیشین صورت پذیرد.

**۱۷- انتشار/بایگانی:** انتشار نرم‌افزار برای تولید یا برای وب، به اتمام فرایند چرخه توسعه نرم‌افزار مشروط است. مشاور امنیتی اختصاص یافته برای هر فرایند انتشار، باید تضمین کند که تیم پروژه الزامات امنیتی رضایت بخشی دارد. مشاور امنیت باید برای تیم پروژه که تمامی الزامات را برآورده می‌سازد، اختصاص داده شود. به طور مشابه برای تمامی محصولات که حداقل دارای یک مولفه با نرخ اثر حریم خصوصی P1 باشند، مشاور حریم خصوصی پروژه باید تایید کند که تیم پروژه تمامی الزامات حریم خصوصی قبل از اینکه اجرا شود را برآورده سازد.

علاوه بر این، تمام داده‌ها و اطلاعات باید برای انجام خدمات پس از انتشار نرم‌افزار، جمع‌آوری شوند که این شامل تمام مشخصات، کد منبع، باینری، نمادها، مدل‌های تهدید، طرح‌های واکنش اضطراری و هرگونه اطلاعات لازم برای انجام وظایف خدماتی پس از انتشار است.

#### **الف-۱۰ ممیزی امنیتی برنامه کاربردی**

**۸-۵-۱ هدف** پنجمین گام از ASMP تایید و ضبط رسمی شواهد پشتیبانی که آیا برنامه کاربردی خاص بدست آمده و یا نگهداری شده در سطح اعتماد هدفمند برنامه کاربردی بوده و یا خیر.

این مرحله از فرایند کاربرد امنیت مدیریتی، می‌تواند در طی کاربرد چرخه حیات انجام شود. براساس سطح اعتماد کاربردی مورد هدف این گام می‌تواند صفر و یک یا دوره‌ای یا لحظه‌ای باشد.

**مثال ۱-** یک سازمان به‌طور دوره‌ای می‌تواند این گام را جهت پایش بر حالت پیاده‌سازی امنیت در طول مرحله تحقق یک برنامه کاربردی انجام دهد.

**مثال ۲-** یک سازمان می‌تواند این گام را برای نشان دادن سطح واقعی میزان اطمینان قبل از اینکه بتواند برای استقرار قابل پذیرش باشد، انجام دهد.

**مثال ۳-** یک سازمان می‌تواند، این گام را در طی مراحل مراحل عملیاتی یک برنامه کاربردی چرخه حیات به‌عنوان بخشی از ممیزی امنیتی سالیانه سازمان انجام دهد.

در این مرحله، تیم داخلی یا خارجی (براساس سیاست‌های سازمانی موجود) و ساختار اصلی سازمان تأیید می‌کند که تمام سنجش‌های فراهم‌شده به‌وسیله کاربرد کنترل‌های امنیتی برای یک کاربرد ویژه، انجام و نتایج آن تأیید شده است. هدف این گام اثبات سطح واقعی امنیت کاربردی در یک زمان خاص است. سازمان می‌تواند یک کاربرد امنیتی را زمانی که سطح واقعی این اعتماد برابر با سطح هدف مورد انتظار باشد، اعلام کند

فرایند ممیزی کاربردهای امنیتی برای سنجش سطح واقعی سطح اعتماد، شماری از افراد و مراحل مختلف را در فرایند توسعه نرم افزار، در بر می گیرد.

- طراحی ویژه‌ای از برنامه‌های کاربردی کسب و کار جهت پیگیری مطابقت با برنامه توسعه نرم افزار و ابزارهای مورد استفاده مدل‌های تهدید استفاده می شود و سایر شواهد خودکار و غیرخودکار ذخیره می شوند.
  - سرپرستان تیم‌های امنیتی و حفظ حریم خصوصی باید اطمینان بدهند که اطلاعات لازم برای بررسی موضوعی جمع آوری شده و از نظر برنامه کاربردی مورد پیگیری قرار گرفتند.
  - این اطلاعات که از نظر کاربردی مورد بررسی قرار گرفتند، به وسیله مشاوران امنیتی و حفظ حریم خصوصی جهت فراهم کردن یک چارچوب برای بررسی امنیتی نهایی (براساس مطالب فوق الذکر)، استفاده می شوند.
  - مشاوران امنیتی و حفظ حریم خصوصی مسئول بررسی اطلاعات وارد شده و پیگیری کاربردی بودن آن (که این شامل بررسی نهایی امنیتی و سایر وظایف امنیتی طرح ریزی شده توسط مشاوران می شود.) و اطمینان از اینکه تمام نیازمندی‌ها و انتظارات حل شده، هستند.
- صفحه نمایش گرفته شده از خط برنامه کاربردی استفاده شده برای ردیابی و تاییدی وظایف امنیت در شکل الف ۴ نشان داده شده است.

Demo for Scoping Questions - Windows Internet Explorer

https://My/DynamicModule.aspx?ModuleId=155&ProjectId=...

Live Search

Questionnaire

I need to...

Home > Dashboard > Project Home > Phase 4: Verification > Tool Compliance

Click to Rate and Give Feedback

### General

Create Project  
Scratch Pad  
Training Reports  
Search  
About

### My

Dashboard  
Settings  
Contact Info  
Training History

### Project Menu

Project Home  
Permissions  
Applicability  
Exception Status  
Fill Out a Survey  
Advisor Only

### Security Advisor

Dashboard  
Exceptions  
Search  
Queue  
Reviews  
Reports

## Tool Compliance: Demo for Scoping Questions

Phase 0 PreReq Phase 1 Req Phase 2 Design Phase 3 Imp Phase 4 Verfy 1 2 3 Phase 5 Release

<< Previous | Next >>

Upload the results of the SDL tools this product is required to run on this page.

#### File Fuzzing

Give feedback on this tool

☐ Check here if none exist

Upload file fuzzing reports for each file extension that requires fuzzing (i.e. - docx, txt, xml, etc.) [?]

Add File Type

Browse... Upload

NO FILE TYPES HAVE BEEN ADDED

Request Exception

#### Have you fuzz tested each file type which requires fuzz testing and corrected issues as described in the [SDL Bug Bar](#)? [?]

☐ Yes ☐ Request Exception Clear

#### RPC Fuzzing

Give feedback on this tool

Upload the report for each RPC interface that 24 hour dumb fuzzing with RPCTest in RPCAttack mode was performed on [?]

Browse... Upload

Request Exception

NO UPLOADED RPC DUMB FUZZING FILES

#### Upload the report for each RPC interface that 24 hour smart fuzzing with RPCVerifier was performed on [?]

Browse... Upload

Request Exception

NO UPLOADED RPC FUZZING FILES

#### ActiveX Fuzzing

Give feedback on this tool

Upload the report for each ActiveX control you fuzzed [?]

Browse... Upload

Request Exception

NO UPLOADED ACTIVE X FUZZING FILES

#### Have you fuzz-tested all ActiveX controls that are marked as either Safe for Scripting or Safe for Initialization with 100+ bad values? [?]

☐ Yes ☐ Request Exception Clear

#### Have all issues identified by ActiveX fuzz testing been corrected as described in the [SDL Bug Bar](#)? [?]

☐ Yes ☐ Request Exception Clear

#### App Verifier

Give feedback on this tool

Has all unmanaged code in the project been tested while running AppVerifier as described in the [SDL AppVerifier Requirements](#)? [?]

☐ Yes ☐ Request Exception Clear

### Recommendations

The below questions are recommendations relevant to this stage of the SDL for your product. These are not SDL requirements and do not affect completion percentage, but certain work items are recommended to improve the security of your product.

Have you used a fuzzing tool on your webservices? [?]	<input type="radio"/> Yes <input type="radio"/> No	<a href="#">Enable</a>
Have you created and completed security testing plans? [?]	<input type="radio"/> Yes <input type="radio"/> No	<a href="#">Enable</a>
Has your product been penetration tested? [?]	<input type="radio"/> Yes <input type="radio"/> No	<a href="#">Enable</a>
Have you developed regression tests for previously known security vulnerabilities? [?]	<input type="radio"/> Yes <input type="radio"/> No	<a href="#">Enable</a>
For online services, have you conducted data flow testing? [?]	<input type="radio"/> Yes <input type="radio"/> No	<a href="#">Enable</a>
For online services, have you conducted replay testing? [?]	<input type="radio"/> Yes <input type="radio"/> No	<a href="#">Enable</a>
Have you followed the <a href="#">SDL Network Protocol Fuzzing Recommendations</a> ? [?]	<input type="radio"/> Yes <input type="radio"/> No	<a href="#">Enable</a>

<< Previous | Next >>

javascript:window.showModalDialog('http://My/...

Local intranet | Protected Mode: Off

95%

شکل الف ۴: مثالی از خط برنامه کاربردی کسب و کار برای ممیزی امنیت برنامه کاربردی



## الف-۱۱ مدل چرخه حیات برنامه کاربردی

۸-۱-۲-۷-۱ سازمانی که کسب و کارش توسعه، برون‌سپاری یا دستیابی به برنامه‌های کاربردی است، از یک چارچوب فرایند تعریف‌شده و فعالیت‌های سازمان‌دهی‌شده در مراحل مختلف استفاده می‌کند. این چارچوب عموماً «مدل چرخه حیات» نامیده می‌شود که براساس زمینه مورد بررسی ممکن است به نام‌های «مدل چرخه حیات برنامه کاربردی»، «مدل چرخه حیات سامانه» یا «مدل چرخه حیات نرم‌افزار» بیان شود.

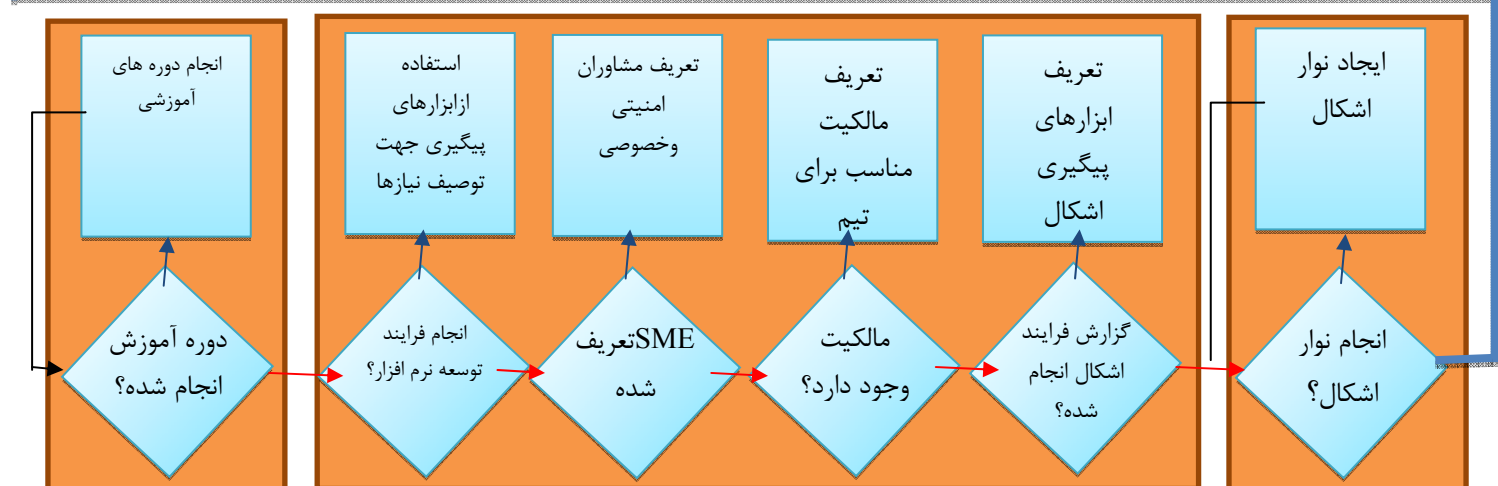
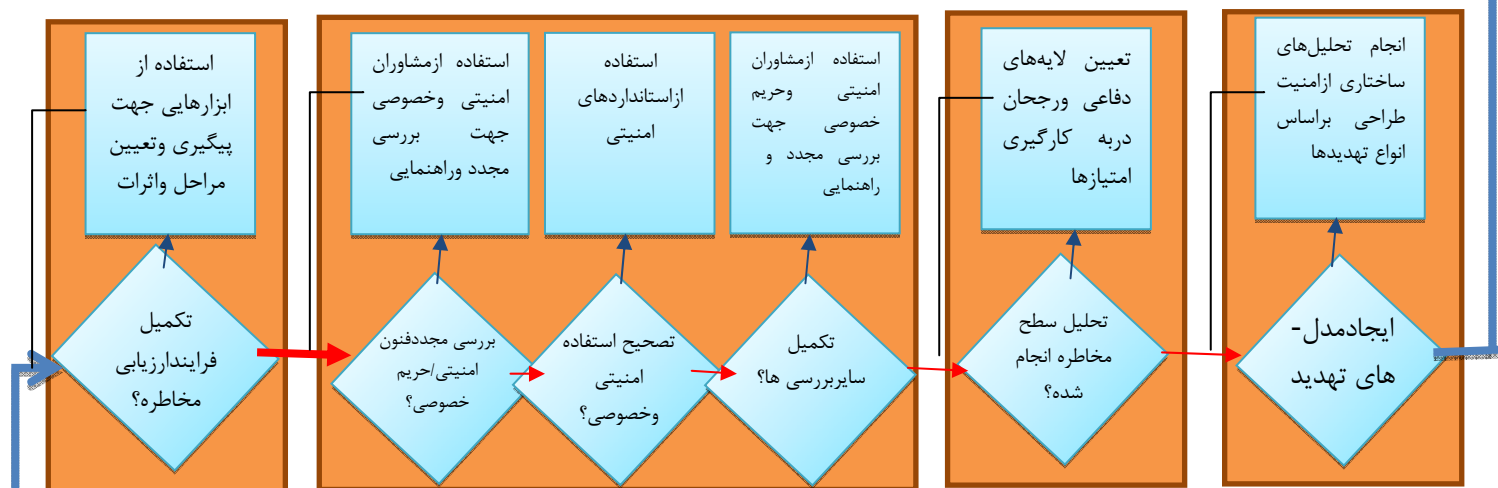
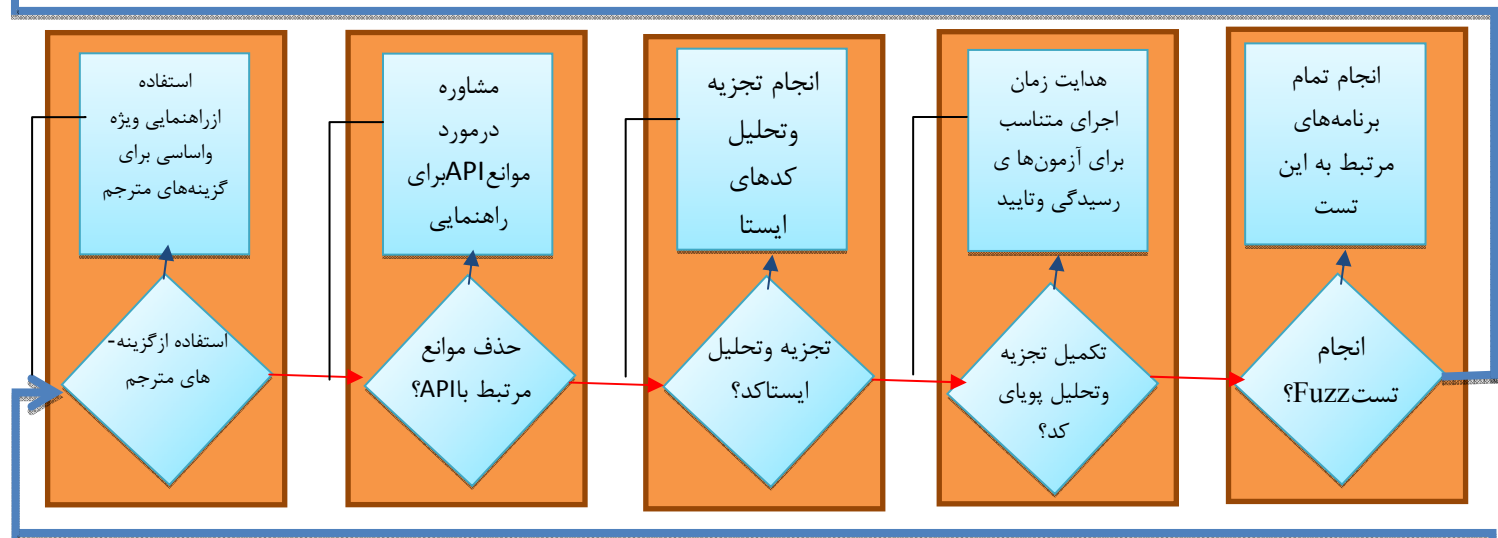
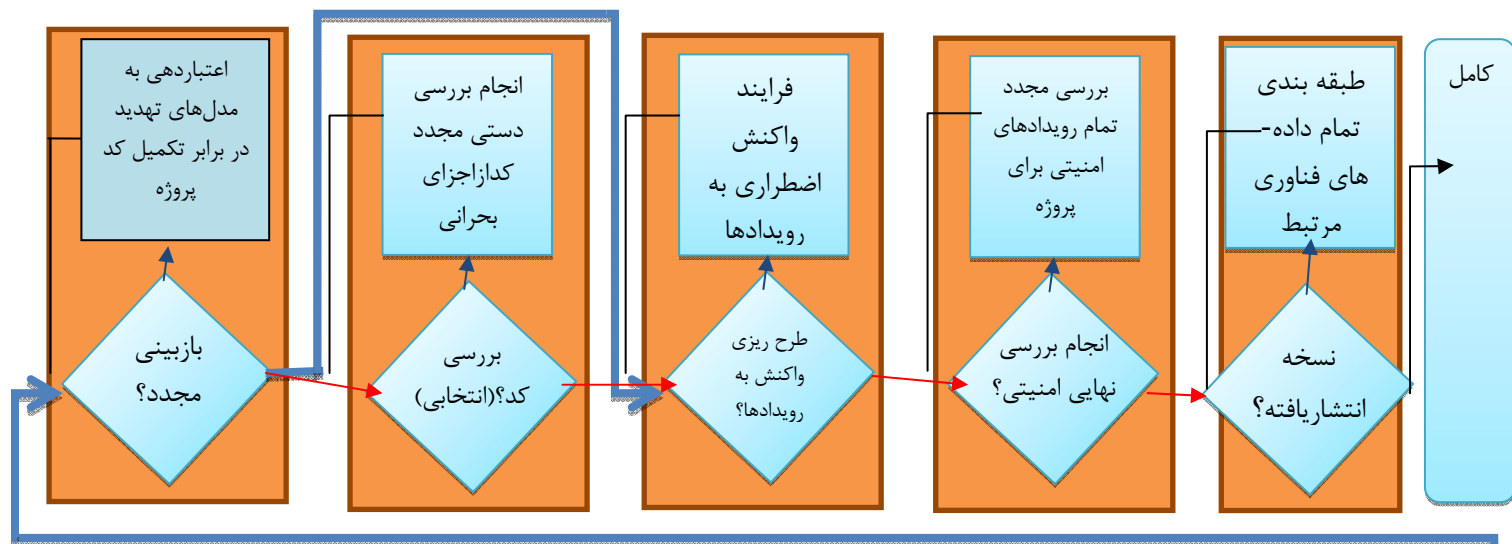
چنین مدلی برای یک سازمان خاص، معمولاً منحصر به فرد و سفارشی است که اغلب برای زمان‌های متعدد در حال استفاده بوده و در طی سال‌ها اصلاح شده است. این مدل به عنوان یک مفهوم جدید که توسط استاندارد بین‌المللی تعریف شود، نیست.

چرخه حیات یک برنامه کاربردی خاص مثلاً تکامل یک برنامه نرم‌افزاری از ابتدا تا انتها معمولاً نمونه‌ای از مدل چرخه حیات است.

گاهی اوقات، گروه‌های مختلفی در داخل یک سازمان پیچیده از مدل‌های متفاوت چرخه حیات برنامه کاربردی برای پروژه‌های کاربردی مختلف استفاده می‌کنند. این اغلب در مورد سازمان‌های بزرگ که از طریق ادغام شکل گرفته‌اند یا غیرمتمرکز نیستند، صدق می‌کند. سازمان‌های دیگر کاربردهای تخصصی و متفاوتی را از مدل‌های چرخه حیات مرتبط با زمینه‌های کاربردی خاص مانند برنامه‌های کاربردی وب، برنامه‌های کاربردی مبتنی بر زمان، برنامه‌های کاربردی پزشکی و ... توسعه می‌دهند.

این مطالعه، کاربرد مدل چرخه حیات، برای نگاشت برنامه‌های امنیتی در فرایند توسعه نرم‌افزار است. سایر بخش‌ها زمینه‌های فنی، کسب و کار و نظارتی و نقشی که در هر یک از زمینه‌ها ایفا می‌شود را طرح‌ریزی می‌کنند.

یک تصویر ساده از فرایند توسعه نرم‌افزار در شکل الف-۵ نمایش داده شده است. این نمودار مشاهده کاربرد کنترل‌های امنیتی مورد استفاده در یک پروژه فرضی از آموزش کارکنان تا مرحله رهایش برنامه‌های کاربردی در یک پروژه فرضی است. این یک نمودار جامع نیست، همان‌طور که قبلاً اشاره شد، بسیاری از تیم‌ها سایر وظایف امنیتی و خصوصی را که مختص برنامه‌های خاص خودشان است را به آن می‌افزایند.

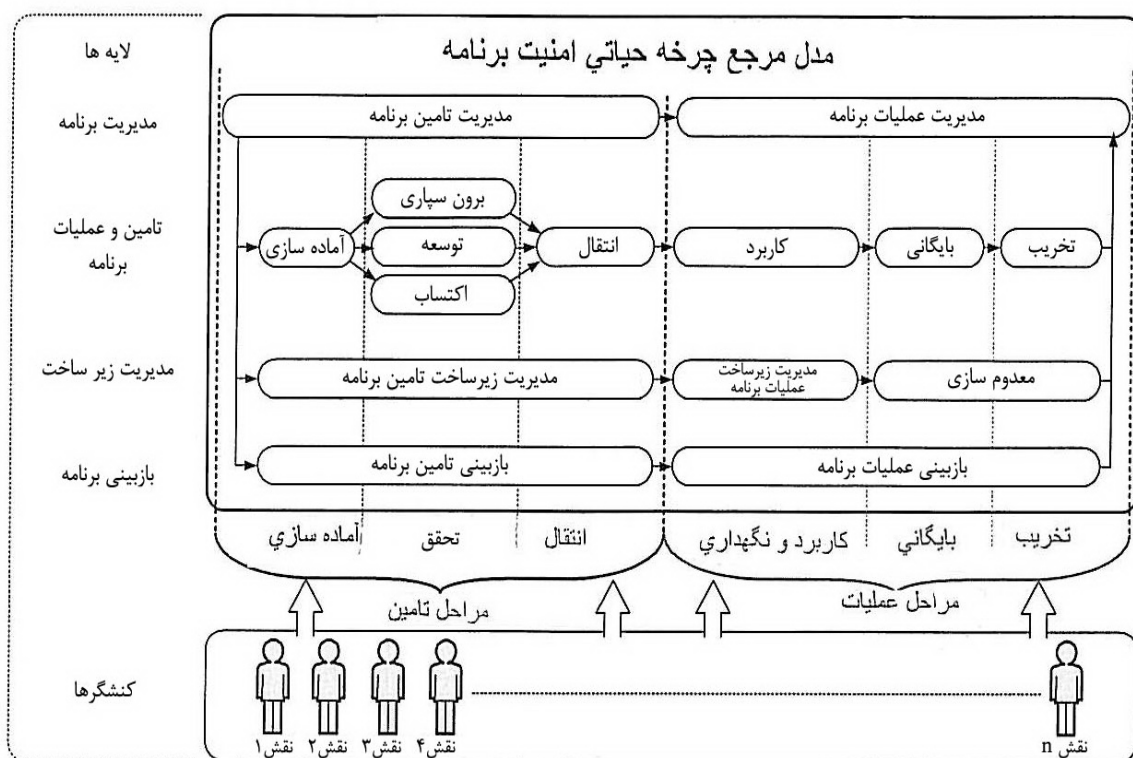


(فلش آبی: No فلش قرمز: Yes)

شکل الف-۵- نمایشی از فرایند SDL

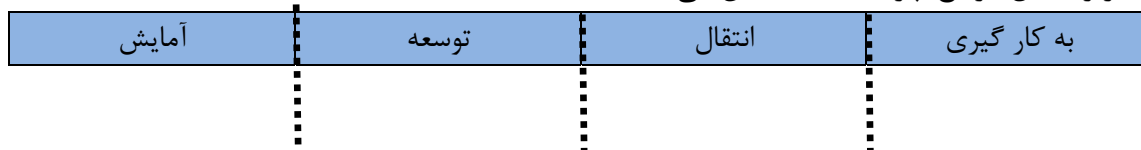
## الف-۱۲ طرح فرایند توسعه نرم افزار بر اساس مدل مرجع چرخه حیات امنیت

فرایند توسعه نرم افزار می تواند براساس مدل مرجع چرخه حیات امنیت برنامه کاربردی که شامل استاندارد ISO/IEC 27034 می شود، طرح ریزی شود. مراحل مدل مرجع توسط فرایند توسعه برنامه کاربردی که به شکل پررنگ شده در شکل الف-۶ نمایش داده شده، پوشش داده می شود:



شکل الف-۶- فرایند توسعه نرم افزار مطابق با چرخه حیات امنیت برنامه کاربردی

به علاوه، شکل الف-۷ جزئیات بیشتری از طرح مراحل فرایند توسعه نرم افزار را براساس مراحل کاربرد مدل مرجع چرخه حیات نشان می دهد.



شکل الف-۷- طرح جزئی مراحل فرایند توسعه نرم افزار با مراحل کاربرد امنیت چرخه حیات مدل مرجع

## مراجع پیوست الف

### زمینه کسب و کار

- i) <http://msdn.microsoft.com/en-us/library/cc307748.aspx>
- ii) <http://msdn.microsoft.com/en-us/library/cc307412.aspx>

### نقش‌ها، وظایف و صلاحیت‌ها

- iii) <http://msdn.microsoft.com/en-us/library/cc307412.aspx>

### بخش مطالعاتی، کاربرد کنترل امنیتی سازمان آموزش

- iv) <http://msdn.microsoft.com/en-us/library/cc307407.aspx>

### نیازمندی‌ها

- V) <http://msdn.microsoft.com/en-us/library/cc307412.aspx>

- vi) <http://msdn.microsoft.com/en-us/library/cc307404.aspx> (امنیت)

- vii) <http://msdn.microsoft.com/en-us/library/cc307403.aspx> (حریم خصوصی)

- viii) <http://msdn.microsoft.com/en-us/library/cc307393.aspx>

- ix) <http://www.microsoft.com/downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&displaylang=en>

### طراحی

- x) <http://msdn.microsoft.com/en-us/library/cc307414.aspx>

- xi) <http://msdn.microsoft.com/en-us/library/cc307415.aspx>

### اجرا

- xii) <http://msdn.microsoft.com/en-us/library/cc307417.aspx>

- xiii) <http://msdn.microsoft.com/en-us/library/cc307395.aspx>

- xiv) <http://msdn.microsoft.com/en-us/library/bb288454.aspx>

- xv) <http://msdn.microsoft.com/en-us/library/cc307395.aspx>

- xvi) <http://msdn.microsoft.com/en-us/library/cc307418.aspx>

- xvii) <http://msdn.microsoft.com/en-us/library/cc307418.aspx>

- xviii) <http://msdn.microsoft.com/en-us/library/cc307408.aspx>

- xix) <http://msdn.microsoft.com/en-us/library/cc307409.aspx>

## پیوست ب

### (اطلاعاتی)

#### نگاشت برنامه کاربردهای کنترل‌های امنیتی با یک استاندارد موجود

**مطالعه موردی: نگاشت برنامه کاربرد کنترل‌های امنیتی توصیف‌شده در NIST SP 800-53 Rev. 3 با کنترل‌های امنیتی توصیف‌شده در استاندارد ISO/IEC 27034.**

هدف این پیوست، توصیف تطبیق کنترل‌های امنیتی از منابع موجود مانند NIST SP 800-53.rev.3 با کنترل‌های امنیتی مورد استفاده و مطابق با استاندارد ISO/IEC 27034 است.

#### **ب-۱) طبقه‌بندی‌های نامزد برنامه کاربرد کنترل‌های امنیت**

این زیربند تلاش می‌کند جنبه‌های احتمالی طبقه‌بندی‌های نامزد کاربرد کنترل‌های امنیتی را که به‌طور مستقیم از SP-800-53 نقل شده است را تعیین کند. سازمان می‌تواند یک طبقه‌بندی از کاربردهای امنیتی مرتبط با امنیت برنامه کاربردی را تعریف کند، مانند:

#### **ب-۱-۱) ملاحظات مرتبط با کنترل‌های امنیت رایج**

کنترل‌های امنیتی تعیین‌شده توسط سازمان به‌عنوان کنترل‌های رایج در اکثر مواقع توسط یک نهاد سازمانی مجزا از دارندگان سامانه‌های اطلاعاتی مدیریت می‌شوند. در فرایند تصمیم‌گیری سازمانی که در آن کنترل‌های امنیتی به‌عنوان کنترل‌های رایج بررسی می‌شوند، می‌تواند تا حد زیادی بر وظایف مالکان سامانه‌های فردی اطلاعاتی، با توجه به اجزای کنترل‌ها در یک مسیر ویژه تأثیر بگذارد. هر کنترلی اساساً باید به‌طور کامل توسط سازمان یا دارندگان سامانه‌های اطلاعاتی تعیین شود.

#### **ب-۱-۲) ملاحظات مرتبط عملیاتی / محیطی**

کنترل‌های امنیتی وابسته به ماهیت محیط اجرا تنها در شرایطی قابل اجرا هستند که سامانه‌های اطلاعاتی در محیطی که کنترل‌ها الزامی است به‌کار گرفته شوند. برای مثال ممکن است برخی از کنترل‌های امنیتی فیزیکی برای سامانه‌های اطلاعاتی مبتنی بر فضا قابل اجرا نباشند و ممکن است کنترل دما و رطوبت برای حس‌گرهای راه دوری که خارج از تجهیزات داخلی حاوی اطلاعات هستند، قابل اجرا نباشند.

#### **ب-۱-۳) ملاحظات مرتبط با زیرساخت فیزیکی**

کنترل‌های امنیتی که اشاره به امکانات سازمانی دارند، (برای مثال، کنترل‌های فیزیکی مثل وجود قفل یا نگهبان و کنترل‌های محیطی برای کنترل دما، رطوبت، نور، آتش و ...) فقط برای آن بخش از امکانات که به‌طور مستقیم وظیفه حفاظت و پشتیبانی را دارند و به سامانه‌های اطلاعاتی مرتبط هستند (شامل اطلاعات فناوری، مثل پست الکترونیکی یا سرویس‌دهنده‌های وب، سرورها، مراکز داده، گره‌های شبکه، دستگاه‌های حفاظتی و وسایل ارتباطی) قابل پذیرش هستند.

#### ب-۱-۴) ملاحظات مرتبط با دسترسی عمومی

از آنجایی که ممکن است برخی کنترل‌های امنیتی از پایه‌های خاص کنترلی (به‌عنوان مثال شناسایی، احراز هویت و کنترل امنیتی کارکنان) برای کاربرانی که از طریق رابط‌های عمومی به سامانه‌های اطلاعاتی دسترسی پیدا می‌کنند، قابل اجرا نباشند، کنترل‌های امنیتی مرتبط با دسترسی عمومی به سامانه‌های اطلاعاتی باید به دقت در نظر گرفته شوند و ملاحظات لازم در آن به کار گرفته شود. برای مثال در حالی که کنترل‌های پایه‌ای شناسایی و احراز هویت کارکنان سازمانی که از سامانه‌های اطلاعاتی تأمین‌کننده خدمات دسترسی همگانی حفاظت و پشتیبانی می‌کنند را لازم می‌داند، ممکن است همین کنترل‌ها برای دسترسی به سامانه‌های اطلاعاتی از طریق رابط‌های همگانی و به‌منظور کسب اطلاعاتی که به شکل همگانی در دسترس هستند، لازم نباشند. از سوی دیگر، شناسایی و احراز هویت برای کاربرانی که از طریق رابط‌های همگانی در برخی موارد، برای مثال برای دسترسی و تغییر اطلاعات شخصی خود استفاده می‌کنند، لازم خواهد بود.

#### ب-۱-۵) ملاحظات مرتبط با فناوری

کنترل‌های امنیتی مربوط به فناوری‌های خاص (به‌عنوان مثال بی‌سیم، رمزنگاری، کنترل‌های عمومی امنیتی و زیرساخت‌های کلیدی عمومی) قابل اجرا هستند، تنها اگر این فناوری‌ها برای به‌کارگیری در سامانه اطلاعاتی به کار گرفته شوند یا مورد نیاز باشند.

کنترل‌های امنیتی تنها در سامانه‌های اطلاعاتی که از قابلیت‌های امنیتی تعیین‌شده به‌وسیله کنترل یا منبع کاهش تهدید بالقوه به‌وسیله کنترل استفاده می‌کنند، قابل اجرا هستند. به‌عنوان مثال وقتی اجزای یک سامانه تک کاربردی هستند، شبکه‌ای نبوده یا فقط مختص شبکه‌های محلی‌اند، یک یا بیش از یک ویژگی منطقی کافی برای عدم پذیرش کنترل‌های انتخاب‌شده توسط اجزا فراهم می‌کنند.

کنترل‌های امنیتی که می‌توانند به صراحت یا به‌طور ضمنی توسط سازوکارهای خودکار حمایت شوند، در صورتی که سازوکاری وجود نداشته باشد یا به آسانی در محصولات تجاری یا دولتی در دسترس نباشد، نیاز به توسعه این چنین سازوکارهایی ندارند. در شرایطی که سازوکارهای خودکار به راحتی در دسترس نباشند، مقرون به صرفه نبوده و یا از نظر فنی امکان‌پذیر نباشد؛ جبران کنترل‌های امنیتی از طریق اجرای سازوکار-های غیرخودکار یا روش‌هایی جهت برآوردن کنترل‌های امنیتی یا پیشرفت‌های کنترلی باید انجام شود. شرایط و ضوابط استفاده از کنترل‌های جبرانی در زیر را ملاحظه فرمایید.

#### ب-۱-۶) ملاحظات سیاسی / نظارتی

کنترل‌های امنیتی که موضوعاتی را به‌وسیله قوانین قابل اجرا، دستورات اجرای دستورالعمل‌ها، کنترل، سیاست‌ها، استانداردها یا قوانین و مقررات (به‌عنوان ارزیابی تأثیر حفظ حریم خصوصی) تعیین می‌کنند، تنها در صورتی الزامی هستند که به‌کارگیری این کنترل‌ها سازگار با انواع اطلاعات و سامانه‌های اطلاعاتی تحت پوشش قوانین قابل اجرا، دستورات اجرایی، دستورالعمل‌ها، سیاست‌ها، استانداردها یا مقررات باشد.

## ب-۱-۷) ملاحظات مربوط به توانمندی و کارایی

کنترل‌های امنیتی با توجه به وسعت و دقت پیاده‌سازی کنترل‌ها از نظر کارایی قیاس‌پذیر هستند. قدرت توانمندی و کارایی با توجه به طبقه‌بندی امنیتی سامانه اطلاعاتی به‌وسیله FIPS199 مشخص می‌شود. برای مثال یک برنامه احتمالی برای FIPS199 (سامانه اطلاعاتی با تأثیر بالا) می‌تواند بسیار طولانی بوده و حاوی مقدار قابل توجهی از جزئیات پیاده‌سازی آن باشد. در مقابل برنامه احتمالی برای FIPS199 (سامانه اطلاعاتی با تأثیر اندک) می‌تواند به‌طور قابل توجهی کوتاه‌تر بوده و حاوی جزئیات پیاده‌سازی اندکی باشد. سازمان‌ها باید اختیاراتی در پذیرش کنترل‌های امنیتی سامانه‌های اطلاعاتی داشته و به قیاس‌پذیری عوامل در محیط‌های خاص توجه داشته باشند، این روش رویکردهای مقرون به‌صرفه و مبتنی بر مخاطره جهت پیاده‌سازی کنترل‌های امنیتی که منابع زیادی بیش از حد لزوم صرف نمی‌کند را تسهیل می‌بخشد و در عین حال دستیابی به کاهش مخاطره، به اندازه کافی و مناسب فراهم می‌شود.

## ب-۱-۸) ملاحظات مبتنی بر اهداف امنیتی

کنترل‌های امنیتی که به‌طور منحصربه‌فردی از موضوعات محرمانه یا اهداف امنیتی در دسترس، حمایت می‌کند؛ می‌تواند براساس کنترل‌های مربوط به پایین‌ترین سطح، کاهش پیدا کند. (اگر در پایین‌ترین سطح تعیین نشود، یا به شکل مناسبی اصلاح یا حذف شود.) فقط و فقط اگر این تنزیل سطح:

۱) مطابق با طبقه‌بندی امنیتی FIPS199 و مطابق با اهداف امنیتی محرمانه باشد و پیش از تغییر در دسترس باشد.

۲) به وسیله ارزیابی مخاطره سازمانی حمایت شود.

۳) بر اطلاعات امنیتی در سامانه اطلاعاتی اثر نگذارد.

کنترل‌های امنیتی زیر توصیه می‌شود:

۱) کنترل‌های محرمانه شامل:

AC-15, MA-3(3), MP-2(1), MP-3, MP-4, MP-5(1)(2)(3), MP-6, PE-5, SC-4, SC-9

۲) کنترل‌های بررسی صحت و درستی SC-8,

۳) کنترل‌های دسترس‌پذیری:

{SC-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6}

## ب-۲) طبقه‌بندی کنترل‌های امنیتی

این زیربند تلاش می‌کند جنبه‌های احتمالی طبقه‌بندی انتخابی کاربرد کنترل‌های امنیتی که به‌طور مستقیم از SP800-53 Rev.3 نقل می‌شوند را تعیین کند.

جدول ب-۱- طبقه بندی کنترل‌های امنیتی، ذکر شرح و مخفف آن

شناسه	خانواده	شرح	طبقه بندی
AC	Access Control	کنترل دسترسی	فنی
AT	Awareness and Training	آگاهی و آموزش	عملیاتی
AU	Audit and Accountability	ممیزی و حسابرسی	فنی
CA	Certification, Accreditation, and Security Assessments	صدور گواهینامه، اعتباربخشی و ارزیابی امنیت	مدیریتی
CM	Configuration Management	مدیریت پیکربندی	عملیاتی
CP	Contingency Planning	طرح ریزی احتمالی	عملیاتی
IA	Identification and Authentication	شناسایی و احراز اصالت	فنی
IR	Incident Response	پاسخ‌دهی به رخدادها	عملیاتی
MA	Maintenance	نگهداری	عملیاتی
MP	Media Protection	حفاظت رسانه	عملیاتی
PE	Physical and Environmental Protection	حفاظت فیزیکی و محیطی	عملیاتی
PL	Planning	طرح ریزی	مدیریتی
PS	Personnel Security	امنیت شخصی	عملیاتی
RA	Risk Assessment	ارزیابی مخاطره	مدیریتی
SA	System and Services Acquisition	کسب سامانه و خدمات	مدیریتی
SC	System and Communications Protection	حفاظت از سامانه و ارتباطات	فنی
SI	System and Information Integrity	سامانه و یکپارچگی اطلاعات	عملیاتی

ب-۳) زیر مجموعه‌ها در طبقه‌بندی کنترل دسترسی

این زیربند تلاش می‌کند مواردی را تعیین کند که می‌تواند در ایجاد کاربرد کنترل‌های امنیتی مورد استفاده باشد و در ارتباط با کنترل دسترسی مطرح شده و مطابق با SP800-53 Rev.3 باشد.



جدول ب-۲- طبقه‌بندی کنترل امنیتی و خطوط راهنمای کنترل‌های امنیتی برای تأثیرگذاری اندک، متوسط و شدید سامانه‌های اطلاعاتی

نام کنترل				شماره کنترل
بالا	متوسط	اندک	کنترل دسترسی	
	AC-1	AC-1	سیاست کنترل دسترسی و روش‌ها	AC-1
AC-2(1)(2)(3)(4)	AC-2(1)(2)(3)(4)	AC-2	مدیریت حساب	AC-2
AC-3(1)	Ac-3(1)	AC-3	اجرای دسترسی	AC-3
AC-4	AC-4	انتخاب نشده	اجرای جریان اطلاعاتی	AC-4
AC-5	AC-5	انتخاب نشده	تفکیک وظایف	AC-5
AC-6	AC-6	انتخاب نشده	حداقل امتیاز	AC-6
AC-7	AC-7	AC-7	تلاش‌های ورود ناموفق	AC-7
AC-8	AC-8	AC-8	هشدار استفاده از سامانه	AC-8
انتخاب نشده	انتخاب نشده	انتخاب نشده	هشدار ورود قبلی	AC-9
AC-10	انتخاب نشده	انتخاب نشده	کنترل همزمان جلسه	AC-10
AC-11	انتخاب نشده	انتخاب نشده	موانع جلسه	AC-11
AC-12(1)	AC-12	انتخاب نشده	اتمام جلسه	AC-12
AC-13(1)	AC-13(1)	AC-13	نظارت و بررسی - کنترل دسترسی	AC-13
AC-14(1)	AC-14(1)	AC-14	عملیات مجاز، شناسایی و تایید	AC-14
AC-15	انتخاب نشده	انتخاب نشده	نشان خودکار	AC-15
انتخاب نشده	انتخاب نشده	انتخاب نشده	برچسب خودکار	AC-16
AC17(1)(2)(3)(4)	AC-17(1)(2)(3)(4)	AC-17	دسترسی از راه دور	AC-17
AC-18(1)(2)	AC-18(1)	AC-18	محدودیت دسترسی	AC-18
AC-19	AC-19	انتخاب نشده	کنترل دسترسی برای دستگاه‌های قابل جابجایی و انتقال	AC-19
AC-19,AC-20(1)	AC-19,AC-20(1)	AC-20	استفاده از سامانه‌های اطلاعاتی خارجی	AC-20

#### ب-۴) دسترسی جزئی به طبقه‌بندی کنترل

این زیربند ۳ جز از طبقه‌بندی دسترسی به کنترل را همان‌طور که طبق SP800-53 مطرح شد، نشان می‌دهد: AC-1,AC-2,AC-17,AT-1.

خانواده: کنترل دسترسی رده: فناوری

#### ب-۴-۱) AC-1 دسترسی به سیاست کنترلی و فرایندها

کنترل: توسعه سازمان، انتشار و بررسی دوره‌ای/به‌روزرسانی

(۱) دسترسی رسمی و مستند به کنترل سیاست که هدف، دامنه، نقش‌ها، مسئولیت‌ها، تعهد مدیریت، هماهنگی میان نهادهای سازمانی و میزان انطباق را تعیین می‌کند.

(۲) روش‌های مستند و رسمی به‌منظور تسهیل در اجرای سیاست کنترلی دسترسی و کنترل‌های دسترسی وابسته

راهنمایی بیشتر: سیاست کنترل دسترسی و روش‌های سازگار با قوانین قابل اجرا، دستورات اجرایی، دستورالعمل‌ها، سیاست‌ها، مقررات، استانداردها و راهنمایی هستند. سیاست‌های کنترل دسترسی می‌تواند بخشی از سیاست‌های کلی امنیت اطلاعات برای سازمان تلقی شود. فرایندهای کنترل دسترسی می‌توانند به‌طور کلی برای برنامه‌های امنیتی و همچنین برای یک سامانه اطلاعاتی به‌طور خاص، زمانی که مورد نیاز است، توسعه یابند. انتشارات ویژه NIST800-12 راهنمایی در مورد سیاست‌های امنیتی و فرایندها فراهم می‌کند.

اولویت و پایه تخصیص:

توسعه کنترل	Low AC-1	MOD AC-1	High AC-1
-------------	----------	----------	-----------

#### ب-۴-۲) AC-2 مدیریت حساب

کنترل: مدیریت سازمان از سامانه اطلاعاتی، شامل:

- ۱) شناسایی انواع حساب (برای مثال فردی، گروهی یا سامانه)
- ۲) ایجاد شرایطی جهت عضویت در گروه
- ۳) شناسایی کاربران مجاز سامانه اطلاعاتی و تعیین حقوق/ امتیازات دسترسی
- ۴) نیاز به مصوبات مناسب برای درخواست ایجاد حساب
- ۵) تأیید، ایجاد، فعال کردن، اصلاح، غیرفعال کردن و از بین بردن حساب
- ۶) بررسی مجدد حساب‌ها (وظیفه تعریف سازمان)
- ۷) اختیارات ویژه و نظارت بر استفاده از حساب‌های میهمان/ ناشناس
- ۸) اطلاع‌رسانی به مدیران حساب وقتی کاربران سامانه اطلاعاتی انتقال و تغییر می‌یابند، یا سامانه‌های اطلاعاتی مورد استفاده قرار می‌گیرند یا تغییرات دیگری رخ می‌دهد.
- ۹) اعطای دسترسی به سامانه اطلاعاتی براساس:

الف) اطلاعات معتبر که به‌وسیله وظایف رسمی اتخاذ شده تعیین می‌شوند و ایجاد رضایت در مورد

معیارهای امنیتی شخصی

ب) استفاده از سامانه در نظر گرفته شده

سایر رهنمودها:

شناسایی کاربران مجاز سامانه اطلاعاتی و تعیین دسترسی به حقوق/ امتیاز مطابق با الزاماتی که در سایر کنترل‌های امنیتی در برنامه‌های امنیتی است. کنترل‌های مرتبط:

AC-1, AC-3, AC-4, AC-5, AC-6, AC-10, AC-13, AC-17, AC-19, AC-20, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SI-9, SC-13

توسعه کنترل:

- ۱) سازمان سازوکارهای خودکار را جهت حمایت از مدیریت حساب سامانه اطلاعاتی به کار می‌گیرد.

- (۲) سامانه اطلاعاتی این سامانه به‌طور خودکار حساب‌های موقت و اضطراری را پس از واگذاری بررسی می‌کند. سازمان یک دوره زمانی برای هر نوع حساب تعیین می‌کند.
- (۳) سامانه اطلاعاتی به‌طور خودکار حساب‌های غیر فعال را از کار می‌اندازد [تخصیص: دوره زمانی تعیین شده‌ی سازمان].
- (۴) سامانه اطلاعاتی به‌طور خودکار ایجاد حساب، اصلاح، غیرفعال بودن، اقدامات فسخ و... را الزاماً توسط افراد مناسب ممیزی می‌کند.
- (۵) سازمان حساب‌های فعال و جاری سامانه اطلاعاتی را بررسی می‌کند، [تخصیص: بازه زمانی تعیین شده‌ی سازمان] جهت تأیید حساب‌های موقت و منقضی‌شده یا انتقال کاربرانی که مطابق با سیاست‌های سازمانی غیرفعال شده‌اند.
- (۶) سازمان استفاده از شناسه‌های حساب، سامانه‌های اطلاعاتی را به‌عنوان شناسه‌ای برای حساب‌های پست الکترونیکی کاربران ممنوع کرده است.

اولویت و پایه تخصیص:

سطح بالا AC-2 (1)(2)(3)(4)(5)(6)	سطح متوسط AC-2 (1) (2) (3) (4) (5) (6)	سطح پایین AC-2
-------------------------------------	---	-------------------

ب-۴-۳) AC-17 دسترسی از راه دور

کنترل: سازمان

- (۱) اسناد، روش‌های دسترسی از راه دور به سامانه اطلاعاتی را مجاز می‌داند.
  - (۲) ایجاد محدودیت در استفاده و راهنمای پیاده‌سازی برای هر یک از روش‌های دسترسی از راه دور
  - (۳) اجازه دسترسی از راه دور به سامانه اطلاعاتی قبل از اتصال
  - (۴) الزامات مورد نیاز اتصال از راه دور به سامانه اطلاعاتی
- راهنمایی تکمیلی: دسترسی از راه دور یک دسترسی به سامانه اطلاعات سازمانی به‌وسیله کاربر (اقدام پردازش از طرف یک کاربر) است که ایجاد ارتباط به‌وسیله شبکه خارجی و شبکه غیرسازمانی تحت کنترل (برای مثال اینترنت) صورت می‌گیرد. مثال‌هایی از دسترسی از راه دور شامل خطوط تلفن، پهنای باند و بدون سیم است. شبکه خصوصی مجازی زمانی که به اندازه کافی تأمین‌شده، ممکن است به‌عنوان یک شبکه کنترل سازمانی تلقی شود. با توجه به ارتباط بدون سیم، سیگنال‌ها در سازمان، تجهیزات را تحت کنترل دارند و به‌طور معمول به‌عنوان کنترل خارج سازمانی تلقی می‌شوند. فناوری‌های بدون سیم محدود به ماکروویو، ماهواره، بسته‌های رادیویی (UHF/VHF) و بلوتوث نیستند. کنترل‌های دسترسی از راه دور برای سامانه‌های اطلاعاتی از طریق سرورهای وب عمومی یا سامانه‌های خاصی که برای دسترسی عمومی طراحی شده‌اند، قابل اجرا هستند. اعمال محدودیت‌های دسترسی به سامانه‌های اطلاعاتی مرتبط با ارتباطات از راه دور توسط کنترل AC-3 انجام می‌شود. NIST که انتشار ویژه 800-77 است، راهنمایی بر شبکه‌های مجازی خصوصی مبتنی بر IPSEC فراهم می‌کند.

انتشارات NIST، 800-48، 800-97 راهنمایی در مورد امنیت شبکه‌های بدون سیم ارائه می‌کنند. انتشار ویژه 800-94 راهنمایی در مورد تشخیص نفوذ و پیشگیری انتشار بدون سیم فراهم می‌کند که کنترل‌های مرتبط با آن AC-1، AC-3، AC-20، IA-2، IA-8 هستند.

#### بهبودهای کنترل:

- ۱) سازمان سازوکارهای خودکار جهت تسهیل نظارت و کنترل روش‌های دسترسی از راه دور به کار می‌گیرد.
- ۲) سازمان از رمزنگاری جهت محافظت از محرمانه بودن و تمامیت دسترسی از راه دور کنترلی، استفاده می‌کند.
- بهبود راهنمایی‌های تکمیلی: قدرت رمزنگاری سازوکار براساس FIPS199 انتخاب می‌شود که بر سطوح اطلاعات تأثیر می‌گذارد. (کنترل‌های مرتبط: SC-8، SC-9)
- ۳) سامانه‌های اطلاعاتی، دسترسی از راه دور را با مدیریت دسترسی به نقاط کنترلی تعیین می‌کنند.
- ۴) سازمان اجازه دسترسی از راه دور را برای دستورات امتیازی و اطلاعات مبتنی بر امنیت فقط برای نیازهای عملیاتی فوری و اسنادی که مبنای دسترسی به طرح‌های امنیتی سامانه اطلاعاتی هستند، ارائه می‌دهد.
- راهنمایی تکمیلی: کنترل مرتبط: AC-6
- ۵) سامانه‌های اطلاعاتی از دسترسی‌های بدون سیم به سامانه با استفاده از احراز هویت و رمزبندی حفاظت می‌کنند.
- راهنمایی تکمیلی: معمولاً برای کاربر، دستگاه یا هر دو در صورت لزوم اعمال می‌شود.
- ۶) نظارت سازمان برای ارتباطات از راه دور غیرمجاز به سامانه‌های اطلاعاتی شامل دسترسی به نقاط غیرمجاز بدون سیم. (سازمان فرکانسی را تعریف کرده و اگر یک ارتباط غیر مجاز کشف شود، عمل مناسبی انجام می‌دهد.)
- راهنمایی تکمیلی: سازمان فعالانه برای ارتباطات غیرمجاز از راه دور بررسی می‌کند، که از جمله شامل بررسی دسترسی به نقاط بدون سیم غیرمجاز می‌شود. این بررسی لزوماً محدود به مناطقی که شامل تسهیلات سامانه‌های اطلاعاتی هستند، نیست؛ بلکه مرتبط با مناطقی خارج از آنها نیز می‌شود که جهت تأیید این که دسترسی به نقاط بدون سیم غیرمجاز تنها محدود به این سامانه‌ها نیست، نیاز به بررسی دارند.
- ۷) سازمان، زمانی که قابلیت‌های شبکه بدون سیم داخلی تعبیه شده در داخل سامانه اطلاعاتی، برای استفاده در نظر گرفته نشود، غیرفعال می‌شود.
- ۸) سازمان به کاربران اجازه نمی‌دهد که به طور مستقل، قابلیت‌های شبکه‌های بدون سیم را شکل‌بندی کنند.

۹) سازمان تضمین می‌کند که کاربران از اطلاعات سازوکارهای دسترسی از راه دور در مورد استفاده و افشای غیرمجاز، محافظت می‌کنند.

۱۰) سازمان کنترل‌های از راه دور را برای دسترسی تضمین می‌کند (فهرستی از عملکردهای امنیتی و اطلاعات مبتنی بر امنیت را تعریف می‌کند). و سنجش‌های دیگری را جهت برقراری امنیت به کار می‌گیرد (تعریف سنجش‌های امنیتی توسط سازمان) و ممیزی می‌کند.

۱۱) سازمان قابلیت‌های بدون سیم شبکه‌ای را در داخل سامانه‌های اطلاعاتی، به جز برای اجزای مشخص شده در حمایت از نیازهای خاص عملیاتی به‌طور صریح، غیرفعال می‌کند.

۱۲) سازمان قابلیت‌های شبکه‌ای بدون سیم (بلوتوث) را در داخل سامانه‌های اطلاعاتی به جز برای اجزای مشخص شده در حمایت از نیازهای خاص عملیاتی به‌طور صریح، غیرفعال می‌کند.

اولویت و پایه تخصیص:

سطح بالا AC-17(1)(2)(3)(4)(5)(6)	سطح متوسط AC-17(1)(2)(3)(4)(5)	سطح پایین AC-17
-------------------------------------	-----------------------------------	--------------------

#### ب-۵) تعریف کاربرد کنترل امنیتی از نمونه کنترلی SP800-53

این بخش به شیوه‌ای غیر رسمی بیان می‌کند که چگونه کنترل AU-14 از SP800-53 می‌تواند از کاربرد کنترل امنیتی ساختار استاندارد ISO/IEC 27034 استفاده کند. ساختار کامل و دقیق داده‌های کاربرد کنترل امنیتی در استاندارد ISO/IEC 27034-5 مورد بحث قرار گرفته است.

ب-۵-۱) کنترل AU-14 توصیف شده در SP800-53 Rev.3 به شکل زیر است:

بخش ممیزی AU-14

کنترل: سامانه اطلاعاتی قابلیت‌های زیر را فراهم می‌کند:

الف) ضبط و ثبت و ورود تمامی مطالب مرتبط به کاربر

ب) بررسی از راه دور تمام مطالب مرتبط با ایجاد جلسات کاربری در زمان واقعی

تکمیل بخش راهنما: فعالیت‌های جلسات ممیزی مطابق با قوانین قابل اجرا، دستورات اجرایی، دستور العمل - ها، سیاست‌ها و مقررات توسعه می‌یابند، یکپارچه می‌شوند و استفاده می‌گردند. بهبود کنترل:

۱) سامانه اطلاعاتی، جلسات ممیزی را در راه‌اندازی سامانه آغاز می‌نماید.

مرجع : ندارد

اولویت و پایه تخصیص

سطح بالا انتخاب نشده	سطح متوسط انتخاب نشده	سطح پایین انتخاب نشده
-------------------------	--------------------------	--------------------------

ب-۵-۲: بررسی کنترل AU-14 به شکل کاربرد کنترل امنیتی مطابق با استاندارد ISO/IEC 27034

همان‌گونه که در جدول ب-۳ در زیر توصیف شده است، کنترل AU-14 می‌تواند به‌عنوان چرخه توسعه امنیت در تطابق با استاندارد ISO/IEC 27034 تشریح شود:

جدول ب-۳- کنترل SP800-53 توصیف شده طبق کنترل AU-14 و استفاده از استاندارد ملی ISO/IEC27034

ارزش	شرح	زمینه
شناسایی ASC		
جلسه ممیزی	متن: نام ASC	برچسب Id - ASC-AU-14
ASC-AU-14	متن: شماره شناسایی ASC	ASC-AU-14_Id-UID
سامانه اطلاعاتی قابلیت‌های زیر را فراهم می‌کند: الف) ضبط و ثبت و ورود کلیه مطالب مرتبط با جلسات کاربر ب) بررسی از راه دور تمام مطالب مرتبط با جلسه ایجاد کاربر در زمان واقعی راهنمایی تکمیلی: فعالیت‌های ممیزی جلسات توسعه یافته، یکپارچه شده و در مشاوره با وکیل استفاده می‌شود.	متن: توصیف ASC در متن ساده	توصیف-Id-ASC-AU-14
Webu, Daming	متن: نام، نام خانوادگی، نام پدر	نام پدیدآورنده Id-ASC-AU-14
شرکت ACME	متن:	نام شرکت پدیدآورنده Id-ASC-AU-14
Wdaming@ACME.com	متن: آدرس ایمیل	ایمیل نویسنده Id-ASC-AU-14
8947358970734205279067248	متن: نام ASC	امضا نویسنده Id-ASC-AU-14
JTC1/SC27 WG4 27034-1 WD3 01-001	شناسه سازمان	Id-ASC-AU-14 سازمان
2009-04-08	تاریخ: yyyy-mm-dd	Id-ASC-AU-14 تاریخ ایجاد
بی ارزش	منبع ASC یا بدون ارزش	Id-ASC-AU-14 اشاره به منبع
بی ارزش	ASC واحد تبعی: فهرست شناسایی ASC یا بدون ارزش	Id-ASC-AU-14 اشاره به واحد تبعی
مالی	فهرست B: بدون ارزش (تهی) یا دارای مفاد	Id-ASC-AU-14 اشاره به زمینه کسب و کار
قانون خصوصی RE76G7، ماده ۴-۱۱	فهرست R: بدون ارزش (تهی) یا دارای مفاد	Id-ASC-AU-14 اشاره به زمینه نظارتی
بدون ارزش	فهرست T: بدون ارزش یا دارای مفاد	Id-ASC-AU-14 اشاره به زمینه فناوری
نرم‌افزار ایجاد یک جلسه مداوم	ویژگی‌های کاربردی که الزامات امنیتی برای ASC فراهم می‌کند.	Id-ASC-AU-14 مشخصات

متن XML ASC-AU-14 Id	شمای XML ASC: شماره متن	v1.0 Beta
زمینه	شرح	ارزش
اهداف ASC		
سطح اعتماد- ASC-AU-14_Obj	۱ یا n- سطوح اعتماد هدف: که در این سطح اعتماد، ASC فعال بوده و شاید مربوط به سطوح مختلف باشد.	5, 6, 7, 8, 9.
دلیل- ASC-AU-14_Obj	چرا SAC وجود دارد. شناسایی نیازها برای مدیر، سرپرست تیم، تیم توسعه، ممیز و ... همچنین طبق هدف، مختصراً بررسی می-شود چه مواردی ارزیابی خواهد شد.	حصول اطمینان از اینکه کاربر مطابق با قانون حریم خصوصی RF76G7#، ماده ۴-۱۱ و استفاده از سیاست‌های مورد پذیرش سازمان
سطح اعتماد، دلیل- ASC-AU-14_Obj		جلسه ممیزی دارای منابع فشرده بوده و تنها مورد نیاز برنامه‌های کاربردی است که اطلاعات شخصی را با مهارت انجام می‌دهد.
سطح اعتماد، مجموع سطوح ASC-AU-14_Obj	محدوده سطوح اعتماد مورد استفاده سازمان	کنترل‌های ۰،۱،۲،۳،۴،۵،۶،۷،۸،۹
ASC-AU-14 -App Spec. - ComplToReg - Std&BestPractices	استانداردهایی که همراه با ASC هستند. (RUP, ITIL, Cobit, ISO 17799 استاندارد، design pattern name etc)	NIST SP-800-53 Rev. 3, AU-14
فعالیت امنیتی ASC		
ASC-AU-14_secAct- بر چسب	متن: نام فعالیت	پیاده‌سازی جلسه ممیزی، با توجه به سطح امنیتی تأیید شده مراکز مطالعاتی
ASC-AU-14_secAct UID	متن: فعالیت امنیتی شناسایی	ACT-001-JAVA027
ASC-AU-14_secAct توضیح	توضیح کامل فعالیت که شرح وظیفه می‌دهد و توصیف می‌کند فرایند و افرادی که نیاز به اجرا و ارزیابی سنجش دارند.	استفاده از سطح امنیتی پذیرفته شده منابع مطالعاتی جهت اجرای فرایند جلسات ممیزی ایمن در برنامه کاربردی
ASC-AU-14_secAct پیچیدگی	سطح پیچیدگی فعالیت: ساده، استاندارد، پیچیده، بسیار پیچیده	ساده
ASC-AU-14_secAct	نقش موجود در سازمان	توسعه‌دهنده

		نقش افراد
تحقق و پیاده سازی	تحقق و مشارکت	ASC-AU-14_secAct
		مسئولیت پذیری فرد
سطح توسعه دهنده گی	احراز صلاحیت فرد: ارائه کننده شرایط مورد نیاز افراد	ASC-AU-14_secAct
متوسط یا بیشتر		صلاحیت فرد
مرحله توسعه، واحد توسعه فعالیت	مورد هدف قرار دادن یک فعالیت در استاندارد ISO/IEC27034، کاربرد امنیتی مدل مرجع چرخه حیات	ASC-AU-14_secAct
		زمان
بررسی مورد مرتبط JAVA	محصول مصنوعی: نام و شرح محصول مصنوعی تولید شده توسط این فعالیت	ASC-AU-14_secAct
		محصول مصنوعی
برای هر معامله، نیاز به ارسال معاملات ویژه به بخش خدماتی و امنیتی سازمان است. نتایج تست این واحد و مدارک آن در پایان این فعالیت مورد انتظار است.	نتایج مورد انتظار، موقعیت، وضع یا ارزش دقیق محصول مصنوعی	ASC-AU-14_secAct
		نتایج - انتظارات
۱۰ روز/ فرد	هزینه فعالیت: هزینه ای برای اتمام این فعالیت در نظر گرفته می شود. (پول - روز/فرد و ...)	ASC-AU-14_secAct
		هزینه
<b>تایید سنجش ASC</b>		
تایید اجرا و پیاده سازی اجزای جلسات ممیزی		ASC-AU-14_VerfMeas
		بر چسب
.VeM-001-JAVA453		ASC-AU-14_VerfMeas-UID:
تأیید اینکه در مورد هر معامله، معاملات خاص به بخش خدمات امنیتی سازمان فرستاده می شود. تأیید نتایج آزمون واحدها و استراتژی مستندات با موفقیت ارائه می شود.		ASC-AU-14_VerfMeas-
		توضیحات
استاندارد	تأیید پیچیدگی های اندازه گیری: ساده، استاندارد، پیچیده، بسیار پیچیده	ASC-AU-14_VerfMeas-
		پیچیدگی
بازبینی کد	نتایج مورد انتظار، موقعیت، وضع یا ارزش دقیق محصول مصنوعی	ASC-AU-14_VerfMeas-
		نقش فردی
تحقق	تحقق - مشارکت	ASC-AU-14_VerfMeas-



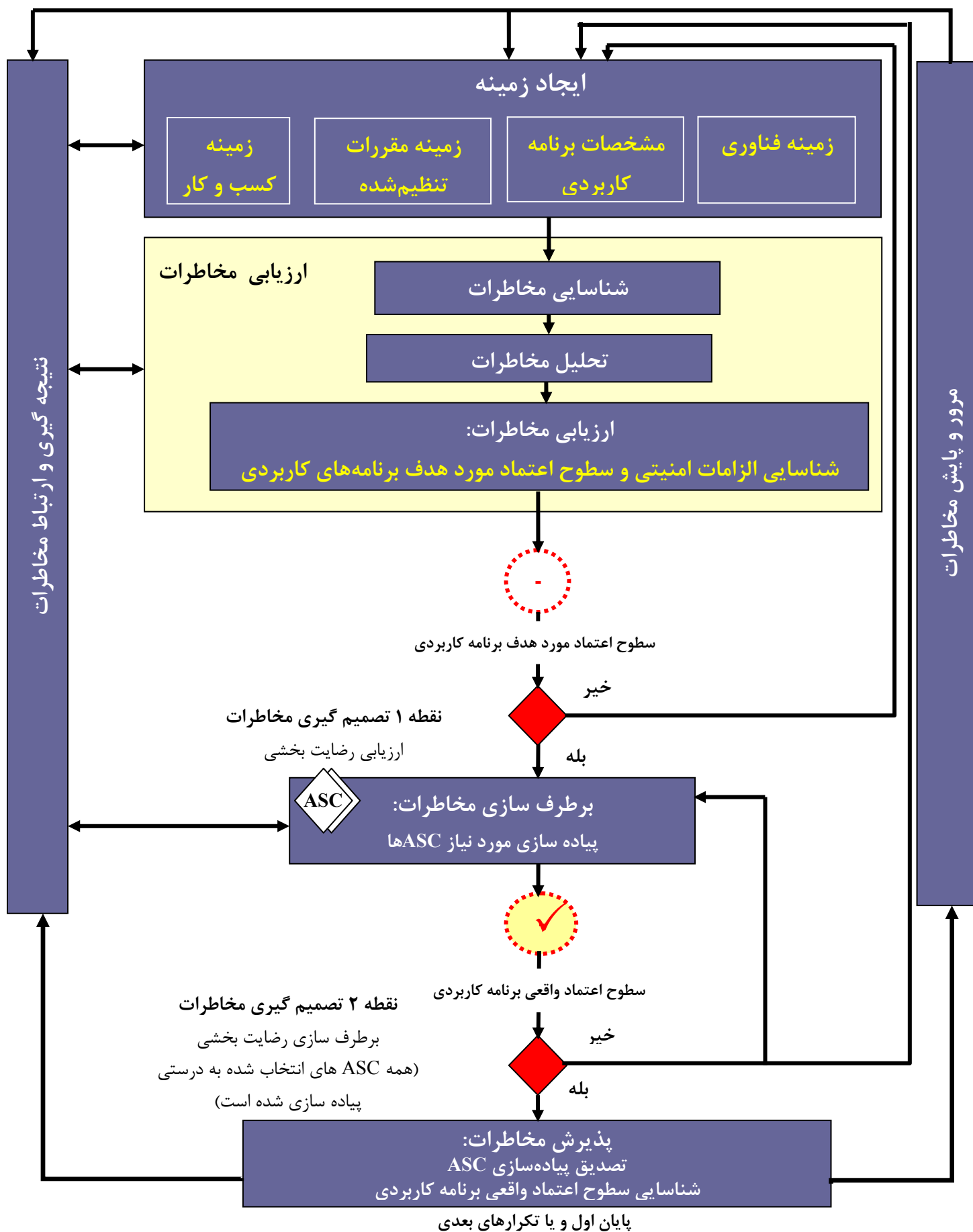
		مسئولیت پذیری
توسعه دهنده JAVA	صلاحیت کنترل فعالیت: ارائه مدارک مورد نیاز افراد	ASC-AU-14_VerfMeas- صلاحیت فردی
مرحله توسعه، فعالیت تست عملکرد	فعالیت مورد هدف در کاربرد امنیتی مدل مرجع چرخه حیات	ASC-AU-14_VerfMeas- زمان - مراحل
نتایج باید برای تمام تأییدهای سنجش صحیح باشد		ASC-AU-14_VerfMeas- محصول فرعی
۱ فرد / روز	بهای تمام شده فعالیت کنترلی: هزینه برای تأیید این فعالیت (فرد/روز، پول و ...) واضح است که ارزیابی دوره‌ای الزامی خواهد بود.	ASC-AU-14_VerfMeas- بهای تمام شده

پیوست پ

(اطلاعاتی)

**فرایند مدیریت مخاطره در استاندارد ملی ایران به شماره 27005 مطابق با فرایند کاربردی  
مدیریت امنیت**

فرایند کاربردی مدیریت امنیت را از نقطه نظر مخاطره در نظر می‌گیریم. بنابراین یک فرایند مشابه  
فرایند مدیریت مخاطره طبق استاندارد ملی ایران به شماره 27005 تعریف می‌شود.



## شکل پ-۱- فرایند مدیریت مخاطره استاندارد ISO/IEC 27005 مطابق با ASMP

عناصر فرایند زیر انجام می‌شوند. در ابتدا چارچوب کاربردی تعیین شده است؛ سپس ارزیابی کاربردی مخاطره سطوح انجام شده است. اگر این موارد اطلاعات کافی برای تعیین کارایی کنترل‌ها فراهم کند، نیاز است که مخاطره سازمان را جهت استفاده از این کاربرد به یک سطح قابل قبول (یا قابل تحمل) کاهش دهیم. سپس این وظیفه تکمیل و راه‌های رفع این مخاطره دنبال می‌شود. اگر اطلاعات ناکافی باشد، ارزیابی مخاطره مجدداً با معیارهای تجدیدنظرشده مخاطره و محیط‌های کاربردی (برای مثال، زمینه کسب و کار، زمینه نظارتی و فناوری، مشخصات کاربردی، معیارهای ارزیابی مخاطره، معیار پذیرش مخاطره، معیارهای تأثیرگذاری و ...) احتمالاً در بخش‌های محدودی از کل برنامه‌های کاربردی تکرار و انجام خواهد شد. اثربخشی رفع مخاطره بستگی به نتایج حاصل از ارزیابی مخاطره دارد. اگر مخاطره و الزامات امنیتی نشأت گرفته برای یک برنامه کاربردی به خوبی مشخص نشود، برنامه کاربردی به اندازه کافی ایمن نخواهد بود؛ زیرا الزامات امنیتی نیاز به شناسایی سطح هدف و میزان اطمینان برنامه کاربردی دارد. امکان‌پذیر است که رفع مخاطره به سرعت منجر به یک سطح مخاطره مورد پذیرش یا قابل تحمل نشود که در آن مورد، تکرار مجدد ارزیابی مخاطره با پارامترهای دقیق‌تر انجام می‌شود. (برای مثال مشخصات برنامه-های کاربردی، نیازمندی‌های امنیتی، سطح اعتماد و کنترل برنامه‌های کاربردی مورد نیاز و ...) اگر لازم باشد، امنیتی مورد پذیرش توسط یک اعتبار رسمی داخلی یا خارجی مورد نیاز است. براساس استاندارد ملی ایران به شماره ۲۷۰۰۵، پذیرش مخاطره در پایان فرایند مدیریت مخاطره انجام می‌شود. زیرا امنیت در یک برنامه کاربردی در پایان مرحله تحقق خود نمی‌تواند پیاده‌سازی شود، توصیه می‌شود پذیرش مخاطره برنامه کاربردی زودتر در فرایند کاربردی مدیریت امنیت توسط صاحب برنامه کاربردی اجرا شود. بهتر است این کار در پایان فرایند ارزیابی مخاطره زمانی که مالک یک سطح هدفمند از میزان اطمینان را برای یک برنامه کاربردی خاص انجام شود. در طول کل فرایند مدیریت مخاطره برنامه کاربردی امنیتی، مهم است که مخاطره، سطح اعتماد و برنامه کاربردی کنترل امنیتی با تیم‌های مناسبی مرتبط باشد. همچنین توصیه می‌شود که صاحب برنامه کاربردی اطمینان حاصل کند که نظارت بر مخاطره و بررسی در طی چرخه حیات برنامه کاربردی انجام می‌شود. آگاهی مدیران و کارمندان سازمان از مخاطره، ماهیت کنترل در مکان جهت حذف مخاطره و مکان‌های نامطمئن در سازمان منجر به مواجهه مناسب در رویدادهای غیرمنتظره با توجه به بهترین حالت می‌شود. همان‌گونه که در استاندارد ملی ایران به شماره ۲۷۰۰۵ تعریف شده، نتایج جزئی در هر بخش از فرایند مدیریت مخاطره و از دو نقطه تصمیم‌گیری مخاطره باید جمع‌آوری شوند.

## کتابنامه

- [1] ISO/IEC 2382-7:2000, *Information technology — Vocabulary — Part 7: Computer programming*
- [2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*
- [3] ISO/IEC 9126 (all parts), *Software engineering — Product quality*
- [4] ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*
- [5] ISO/TS 15000 (all parts), *Electronic business eXtensible Markup Language (ebXML)*
- [6] ISO/IEC 15026 (all parts), *Systems and software engineering — Systems and software assurance*
- [7] ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*
- [8] ISO/IEC 15289:2006, *Systems and software engineering — Content of systems and software life cycle process information products (Documentation)*
- [9] ISO/IEC 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*
- [10] ISO/IEC TR 15443 (all parts), *Information technology — Security techniques — A framework for IT security assurance*
- [11] ISO/IEC 18019:2004, *Software and system engineering — Guidelines for the design and preparation of user documentation for application software*
- [12] ISO/IEC TR 20000-4:2010, *Information technology — Service management — Part 4: Process reference model*
- [13] ISO/IEC 21827:2008, *Information technology — Security techniques — Systems Security Engineering— Capability Maturity Model® (SSE-CMM®)*
- [14] ISO/IEC/IEEE 24765:2010, *Systems and software engineering — Vocabulary*
- [15] ISO/IEC/IEEE 29148 (to be published), *Systems and software engineering — Life cycle processes — Requirements engineering*
- [16] ISO/IEC TR 29193 (under development), *Secure system engineering principles and techniques*
- [17] NIST Special Publication 800-48:2008, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*
- [18] NIST Special Publication 800-53 Revision 3:2009, *Recommended Security Controls for Federal Information Systems and Organizations*
- [19] NIST Special Publication 800-77:2005, *Guide to SSL VPNs*
- [20] NIST Special Publication 800-94:2007, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- [21] NIST Special Publication 800-97:2007, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*