INSOISO-IEC

27034-1

1st. Edition

2015
Identical with
ISO/IEC 27034-1:
2011 + COR1:2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

استاندارد ملی ایران
ایزو-آی‌ای‌سی
۲۷۰۳۴-۱

چاپ اول

۱۳۹۴

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

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به‌موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن‌ماه 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 به‌موجب 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 ابلاغ‌شده است .

تدوین استاندارد در حوزه‌های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود .پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین‌شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و در صورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود .بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته‌شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1] ،کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه‌شناسی قانونی (OIML)[3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور ، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی‌شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به‌منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گران‌بها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

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:	**سمت و/یا نمایندگی**
فولادیان، مجید (فوق لیسانس مهندسی برق مخابرات)	مشاور سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی)	مدیرکل نظام مدیریت امنیت اطلاعات 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

فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فیاضی، مهدی (لیسانس مهندسی برق الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
معروف، سینا (لیسانس مهندسی کامپیوتر- سخت‌افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رییس اداره تدوین استانداردها و نظارت بر امنیت سرویس‌ها سازمان فناوری اطلاعات ایران
موجبی، محمود (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
ناپلیان، کامران (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
ناصری، علی (دکتری برق مخابرات)	عضو هیأت علمی دانشگاه امام حسین (ع)
وکیلی، اسد الله (فوق لیسانس مهندسی کامپیوتر)	مدیر پروژه موسسه تحقیقات ارتباطات و فناوری اطلاعات
ناظمی، اسلام (دکترای مهندسی کامپیوتر نرم‌افزار)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (فوق لیسانس فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی

یعقوبی رفیع، کمال‌الدین پژوهش‌گر دانشگاه شهید بهشتی
(فوق لیسانس فناوری اطلاعات معماری سازمانی)

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد«فناوری اطلاعات- فنون امنیتی- امنیت برنامه کاربردی- قسمت ۱: مرور کلی و مفاهیم»که پیش‌نویس آن در کمیسیون‌های مربوط به‌وسیله سازمان فناوری اطلاعات ایران تهیه و تدوین‌شده و در سیصدو هفتاد و ششمین اجلاس کمیته‌ی ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۴/۰۳/۰۳ مورد تصویب قرارگرفته 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 درزمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهاد که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط موردتوجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تدوین این استاندارد مورداستفاده قرارگرفته به شرح زیر است:

ISO/IEC 27034-1: 2011 + COR1:2014 *Information technology — Security techniques Application security — Part 1: Overview and concepts*

۰ مقدمه

۰-۱ کلیات

برای باقی ماندن در کسب‌وکار، توصیه می‌شود سازمان‌ها از زیرساخت‌های اطلاعاتی و فناورانه خود حفاظت کنند. به‌طور سنتی، این مسئله در سطح فناوری اطلاعات به‌وسیله حفاظت پیرامون و مؤلفه‌های زیرساختی فناورانه مانند رایانه‌ها و شبکه‌ها اداره شده است که به‌طورکلی ناکافی هستند.

علاوه بر این، سازمان‌ها به‌طور فزاینده در سطح حاکمیت با اجرا کردن سامانه‌های مدیریت امنیت اطلاعات (ISMS)[1] رسمی، آزموده شده و درستی‌سنجی‌شده، از خود حفاظت می‌کنند. طبق استاندارد ملی ایران شمارهٔ ۲۷۰۰۱: سال ۱۳۸۷، یک رویکرد نظام‌مند به سامانه مؤثر مدیریت امنیت اطلاعات کمک می‌کند.

بااین‌حال سازمان‌ها با نیاز در حال رشد حفاظت از اطلاعات خویش در سطح برنامه کاربردی روبرو هستند.

توصیه می‌شود برنامه‌های کاربردی در مقابل آسیب‌پذیرهایی که ممکن است مربوط به ذات برنامه کاربردی باشند (برای نمونه نقص‌های 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 نشده است، به وجود می‌آیند، حفاظت شوند.

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، برون‌سپاری یا خرید یک محصول تجاری به دست آیند. برنامه‌های کاربردی همچنین می‌توانند از طریق ترکیب این رویکردها به دست آیند که ممکن است پیامدهای امنیتی جدیدی را ایجاد نمایند که توصیه می‌شود در نظر گرفته‌شده و مدیریت شوند.

نمونه‌هایی از برنامه‌های کاربردی، سامانه‌های منابع انسانی، سامانه‌های مالی، سامانه‌های پردازش واژه، سامانه‌های مدیریت مشتریان، دیوارهای آتش، سامانه‌های ضدویروس و سامانه‌های تشخیص نفوذ است.

یک برنامه کاربردی امن در طول چرخه حیات خود، ویژگی‌های لازم از کیفیت نرم‌افزار مانند اجرای قابل پیش‌بینی و انطباق را نشان می‌دهد و هم‌چنین نیازهای امنیتی از دیدگاه توسعه، مدیریت، زیرساخت فناورانه و ممیزی را برآورده می‌کند. فرایندها و تجارب تقویت‌شده ازنظر امنیت و افراد ماهری که آن‌ها را انجام دهند، برای ساختن برنامه‌های کاربردی قابل‌اطمینانی که در معرض مخاطره قرار گرفتن را از سطح قابل‌قبول و قابل‌تحمل مخاطره باقیمانده افزایش ندهند و از یک ISMS مؤثر پشتیبانی کنند، لازم هستند.

علاوه بر این، یک برنامه کاربردی امن نیازهای امنیتی ناشی از نوع داده‌ها، محیط هدف (زمینه‌های کسب‌وکار، تنظیم مقررات و فنی)، کنشگرها و مشخصات برنامه کاربردی را در نظر می‌گیرد. توصیه می‌شود امکان به دست آوردن شواهدی که مشخص می‌کنند مخاطره باقیمانده در سطح قابل‌قبول (یا قابل‌تحمل) اکتساب‌شده و نگهداری می‌شود وجود داشته باشد.

1- Information security management system

۰-۲ هدف

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

الف- فراهم کردن مفاهیم، اصول، چارچوب‌ها، مؤلفه‌ها و فرایندها؛

ب- فراهم کردن سازوکارهای فرایندگرا برای ایجاد نیازهای امنیتی، ارزیابی مخاطرات امنیتی، اختصاص سطح اعتماد هدف‌گذاری‌شده و انتخاب واپایش‌های امنیتی و سنجه‌های درستی‌سنجی مربوطه؛

پ- فراهم کردن رهنمودهایی برای ایجاد معیارهای پذیرش برای سازمان‌هایی که توسعه یا بهره‌برداری از برنامه‌های کاربردی را برون‌سپاری می‌کنند و برای سازمان‌هایی که برنامه‌های کاربردی طرف سوم را خریداری می‌کنند.

ت- فراهم کردن سازوکارهای فرایندگرا برای مشخص کردن، تولید و جمع‌آوری شواهد موردنیاز برای نشان دادن این‌که برنامه‌های کاربردی آن‌ها می‌توانند به‌طور امن در محیطی تعریف‌شده استفاده شوند.

ث- حمایت از مفاهیم کلی تعیین‌شده در استاندارد ملی ایران به شماره۲۷۰۰۱ : سال ۱۳۸۷ و کمک به پیاده‌سازی رضایت‌بخش امنیت اطلاعات بر پایه رویکرد مدیریت مخاطره؛ و

ج- فراهم کردن چارچوبی که به پیاده‌سازی واپایش‌های امنیتی تعیین‌شده در استاندارد ملی ایران به شماره ۲۷۰۰۲ : سال ۱۳۸۷و دیگر استانداردها کمک کند.

این استاندارد ملی در موارد زیر کاربرد دارد:

الف- در مورد نرم‌افزارهای زیرین از برنامه کاربردی و عامل‌های کمک‌کننده‌ای 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 هراندازه (برای نمونه شرکت‌های تجاری، نهادهای 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 واپایش‌ها یا سنجش‌ها؛

پ- ارائه مشخصات کدگذاری امن برای هرگونه زبان برنامه‌نویسی.

این استاندارد ملی :

الف- استاندارد توسعه نرم‌افزار کاربردی نیست؛

ب- استاندارد مدیریت پروژه برنامه کاربردی نیست؛

پ- استاندارد چرخه حیات توسعه نرم‌افزار نیست.

نیازها و فرایندهای مشخص‌شده 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 گرفته‌شده‌اند. به این منظور

توصیه می‌شود سازمان‌ها فرایندهای موجود و چارچوب‌های پیشنهادشده توسط این استاندارد ملی را نگاشت کند تا تأثیر پیاده‌سازی این استاندارد ملی کاهش یابد.
پیوست الف (اطلاعاتی) نمونه‌ای را فراهم می‌کند که توضیح می‌دهد چگونه یک فرایند توسعه نرم‌افزار موجود می‌تواند به برخی اجزا و فرایندهای این استاندارد ملی نگاشت شود. به‌طورکلی توصیه می‌شود هر سازمانی که از هرگونه چرخه حیات توسعه استفاده می‌کند، نگاشتی مانند نگاشت توصیف‌شده در پیوست الف را انجام دهد و اجزا و فرایندهای جامانده موردنیاز را برای تطبیق با این استاندارد ملی اضافه کند.

۰-۳ مخاطبان هدف

۰-۳-۱ کلیات

مخاطبان زیر در حین اجرای نقش‌های سازمانی تعیین‌شده خود از این استاندارد بهره می‌برند:
الف- مدیران
ب- گروه‌های تامین و عملیات
پ- کارکنان گروه کارفرما
ت- تامین‌کنندگان
ث- ممیزان

۰-۳-۲ مدیران

مدیران افراد درگیر در مدیریت برنامه کاربردی در طی چرخه حیات کامل آن هستند. مراحل کاربردپذیر چرخه حیات برنامه کاربردی، مراحل تامین و تولید را شامل می‌شوند. نمونه‌هایی از مدیران عبارت‌اند از:
الف- مدیران امنیت اطلاعات
ب- مدیران پروژه
پ- راهبران
ت- کارفرمایان نرم‌افزار
ث- مدیران توسعه نرم‌افزار
ج- مالکان برنامه کاربردی
چ- مدیران صف که بر کارکنان نظارت دارند.
به‌طورمعمول لازم است مدیران:
الف- هزینه پیاده‌سازی و حفظ امنیت برنامه کاربردی را در برابر مخاطرات و ارزشی که برای سازمان دارد، متعادل کنند؛
ب- گزارش ممیزهایی که پیشنهاد قبول یا رد برنامه کاربردی را بر اساس این‌که آیا برنامه کاربردی سطح اطمینان هدف‌گذاری شده را اکتساب کرده و حفظ می‌کند بازبینی کنند؛
پ- از سازگاری با استانداردها، قوانین و مقررات مطابق با زمینه مقرراتی برنامه کاربردی اطمینان حاصل کنند. (به بند ۸-۱-۲-۲ مراجعه شود.)
ت- پیاده‌سازی برنامه کاربردی امن را راهبری کنند؛

ث- سطح اعتماد هدف‌گذاری شده را طبق زمینه [کاربرد] خاص سازمان تصویب کنند؛
ج- مشخص کنند کدام‌یک از واپایش‌ها و سنجش‌های درستی‌سنجی، توصیه می‌شود پیاده‌سازی و آزموده شوند؛
چ- هزینه‌های درستی‌سنجی امنیت برنامه کاربردی را به کمینه برسانند؛
ح- خط‌مشی‌ها و رویه‌های امنیتی یک برنامه کاربردی را مستندسازی کنند؛
خ- برای تمام کنشگرها آگاهی، آموزش و دید آگاهانه امنیتی فراهم کنند؛
د- اختیارات امنیت اطلاعات مناسب موردنیاز خط‌مشی‌ها و رویه‌های امنیت اطلاعات کاربردپذیر را جایگذاری کنند؛ و
ذ- در تمام طرح‌های امنیتی مربوط به سامانه در سرتاسر شبکه سازمان حضورداشته باشند.

۰-۳-۳ گروه‌های تامین و عملیات

اعضای گروه‌های تامین و عملیات (که درمجموع به‌عنوان گروه پروژه شناخته می‌شوند.) افرادی درگیر در طراحی، توسعه و نگهداری برنامه کاربردی در طول چرخه کامل حیات آن هستند. این افراد عبارت‌اند از:
الف- معماران،
ب- تحلیل‌گران،
پ- برنامه‌نویسان،
ت- آزمایش‌کنندگان،
ث- راهبران سامانه،
ج- راهبران دادگان،
چ- راهبران شبکه و
ح- کارکنان فنی.
به‌طورمعمول لازم است اعضا:
الف- درک کنند کدام واپایش‌ها توصیه می‌شود در هر مرحله از چرخه حیات برنامه کاربردی به کار گرفته - شوند و چرا؛
ب- درک کنند کدام واپایش‌ها توصیه می‌شود در خود برنامه کاربردی پیاده‌سازی شوند؛
پ- تأثیر معرفی واپایش‌ها را در فعالیت‌های توسعه، آزمایش و مستندسازی در چرخه حیات برنامه کاربردی به کمینه برسانند؛
ت- اطمینان حاصل کنند که واپایش‌های معرفی‌شده نیازهای سنجش‌های مربوطه را برآورده می‌کنند؛
ث- به‌منظور مؤثر کردن توسعه، آزمایش و مستندسازی،به ابزارها و بهترین تجارب دسترسی پیدا کنند؛
ج- بازبینی گروهی را آسان کنند؛
چ- در برنامه‌ریزی و تهیه راهبرد شرکت کنند؛
ح- برای اکتساب کالاها و خدمات موردنیاز (برای نمونه درخواست، ارزیابی و اعطای قراردادها) روابط کسب‌وکار را ایجاد کنند؛ و

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

۰-۳-۴ کارفرمایان

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

به‌طورکلی لازم است کارفرمایان:

الف- درخواست‌های پیشنهادها که شامل نیازهای واپایش‌های امنیتی است را آماده کنند؛

ب- تامین‌کنندگان سازگار با این نیازها را انتخاب کنند؛

پ- شواهد واپایش‌های امنیتی به کار گرفته‌شده توسط خدمات برون‌سپاری را درستی‌سنجی کنند؛ و

ت- محصولات را با درستی‌سنجی شواهد پیاده‌سازی صحیح واپایش‌های امنیت برنامه کاربردی ارزیابی کنند.

۰-۳-۵ تامین‌کنندگان

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

به‌طورکلی لازم است تامین‌کنندگان:

الف- از نیازهای امنیتی برنامه کاربردی در درخواست‌های پیشنهادها پیروی کنند؛

ب- واپایش‌های امنیتی برنامه کاربردی مناسب را با توجه به تأثیر آن‌ها بر هزینه‌ها برای پیشنهادها انتخاب کنند؛

پ- شواهدی فراهم کنند مبنی بر این‌که واپایش‌های امنیتی موردنیاز به‌درستی در محصولات یا خدمات پیشنهادی پیاده‌سازی شده‌اند؛

۰-۳-۶ ممیزها

ممیزها افرادی هستند که لازم است:

الف- محدوده و رویه‌های درگیر در سنجش‌های درستی‌سنجی برای واپایش‌های مرتبط را درک کنند؛

ب- اطمینان حاصل کنند که نتایج ممیزی تکرارپذیر هستند؛

پ- فهرستی از سنجش‌های درستی‌سنجی که شواهدی مبنی بر رسیدن برنامه کاربردی به سطح اعتماد هدف‌گذاری شده‌ی موردنیاز توسط مدیریت تولید می‌کند را ایجاد کنند ؛ و

ت- فرایندهای ممیزی استاندارد را بر پایه استفاده از شواهد قابل درستی‌سنجی به‌کارگیرند.

۰-۳-۷ کاربران

کاربران افرادی هستند که لازم است:

الف- اعتماد داشته باشند که استفاده یا استقرار برنامه کاربردی، امن فرض می‌شود؛

ب- اعتماد داشته باشند که یک برنامه کاربردی نتایج اطمینان‌پذیری را به شکل مداوم و به‌موقع تولید می‌کند؛

پ- اعتماد داشته باشند که واپایش‌ها و سنجش‌های درستی‌سنجی مرتبط به شکل صحیح و طبق انتظار قرارگرفته و کار می‌کنند.

۰-۴ اصول

۰-۴-۱ امنیت یک الزام است

توصیه می‌شود نیازهای امنیتی برای هر مرحله از چرخه حیات یک برنامه کاربردی تعریف و تحلیل شوند، به‌درستی مورد خطاب قرار گیرند و به شکل پیوسته مدیریت شوند.

توصیه می‌شود با نیازهای امنیتی برنامه کاربردی (به بند ۶-۴ مراجعه شود) به همان شیوه برخورد با نیازهای کارکرد، کیفیت و کاربردپذیری (برای نمونه‌ای از مدل کیفیت به استاندارد ISO/IEC 9126 مراجعه شود) برخورد کرد. علاوه بر این، توصیه می‌شود نیازهای مرتبط با امنیت برای مطابقت با محدودیت‌های به وجود آمده در مخاطرات باقیمانده، برقرار شوند.

مطابق با استاندارد ISO/IEC/IEEE 29148 (در حال تدوین)، توصیه می‌شود نیازهای ضروری، چکیده، غیر مبهم، سازگار، کامل، دقیق، امکان‌پذیر، قابل‌ردیابی و وارسی پذیر باشند. توصیه می‌شود ویژگی‌های مشابه در مورد نیازهای امنیتی به کار گرفته شوند. اغلب اوقات در مستندات پروژه‌های برنامه کاربردی با نیازهای امنیتی مبهم مانند «توسعه‌دهنده باید تمام مخاطرات امنیتی مهم در برنامه کاربردی را کشف کند» مواجه می‌شویم.

۰-۴-۲ امنیت برنامه کاربردی وابسته به زمینه [کاربرد] است

امنیت برنامه کاربردی تحت تأثیر محیط هدف تعریف‌شده است. نوع و محدوده نیازهای 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 کسب‌وکار: مخاطرات خاص برخاسته از زمینه کسب‌وکار سازمان (شرکت مخابرات، شرکت حمل‌ونقل، دولت و غیره)؛

ب- زمینه مقرراتی: مخاطرات خاص برخاسته از مکان جغرافیایی که سازمان در آن مشغول کسب‌وکار است. (حقوق و سند مالکیت فکری، محدودیت‌های حفاظت رمزنگاری، حق نشر[1]، قوانین و مقررات، قانون حریم خصوصی و غیره)؛

پ- زمینه فناورانه: مخاطرات خاص از فناوری‌های استفاده‌شده توسط سازمان در جریان کسب‌وکار[مهندسی معکوس، امنیت ابزارهای ساخت، حفاظت از کد منبع، استفاده از کد از پیش تفسیر شده طرف سوم، آزمایش امنیت، آزمایش نفوذ، بررسی حدود، بررسی کد، محیط فناوری اطلاعات و ارتباطات (ICT) که برنامه کاربردی در آن اجرا می‌شود، فایل‌های پیکربندی و داده‌های تفسیرنشده ، اولویت‌های سامانه عامل برای نصب یا بهره‌برداری ، نگهداری و توزیع امن و غیره.]

زمینه فناورانه مشخصات فنی برنامه کاربردی را دربر می‌گیرد (کارکرد امنیتی، اجزای من، پرداخت برخط، رویداد نگاشت[2] من، رمزنگاری، مدیریت مجوزها و غیره.)

1- Copyright
2- Log

یک سازمان می‌تواند تأیید کند که یک برنامه کاربردی امن است اما این تأیید تنها برای این سازمان و در حوزه کسب‌وکار، مقرراتی و فنی خاص آن معتبر است. چنانچه برای مثال زیرساخت فناورانه برنامه کاربردی تغییر کند یا برنامه کاربردی با همین مقصود در کشور دیگری استفاده شود، ممکن است این حوزه‌های جدید بر نیازهای امنیتی و سطح اعتماد هدف‌گذاری شده تأثیر بگذارند. ممکن است واپایش‌های امنیتی برنامه کاربردی، دیگر به‌درستی نیازهای امنیتی جدید را مورد خطاب قرار ندهند و ممکن است برنامه کاربردی دیگر امن نباشد.

۰-۴-۳ سرمایه‌گذاری مناسب برای امنیت برنامه کاربردی

توصیه می‌شود هزینه‌های اعمال واپایش‌های امنیت برنامه کابردی و انجام سنجش‌های ممیزی با سطح اعتماد هدف‌گذاری شده (به بند ۸-۱-۲-۶-۴ مراجعه شود) موردنیاز توسط مالک برنامه کاربردی یا مدیریت متناسب باشد.

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

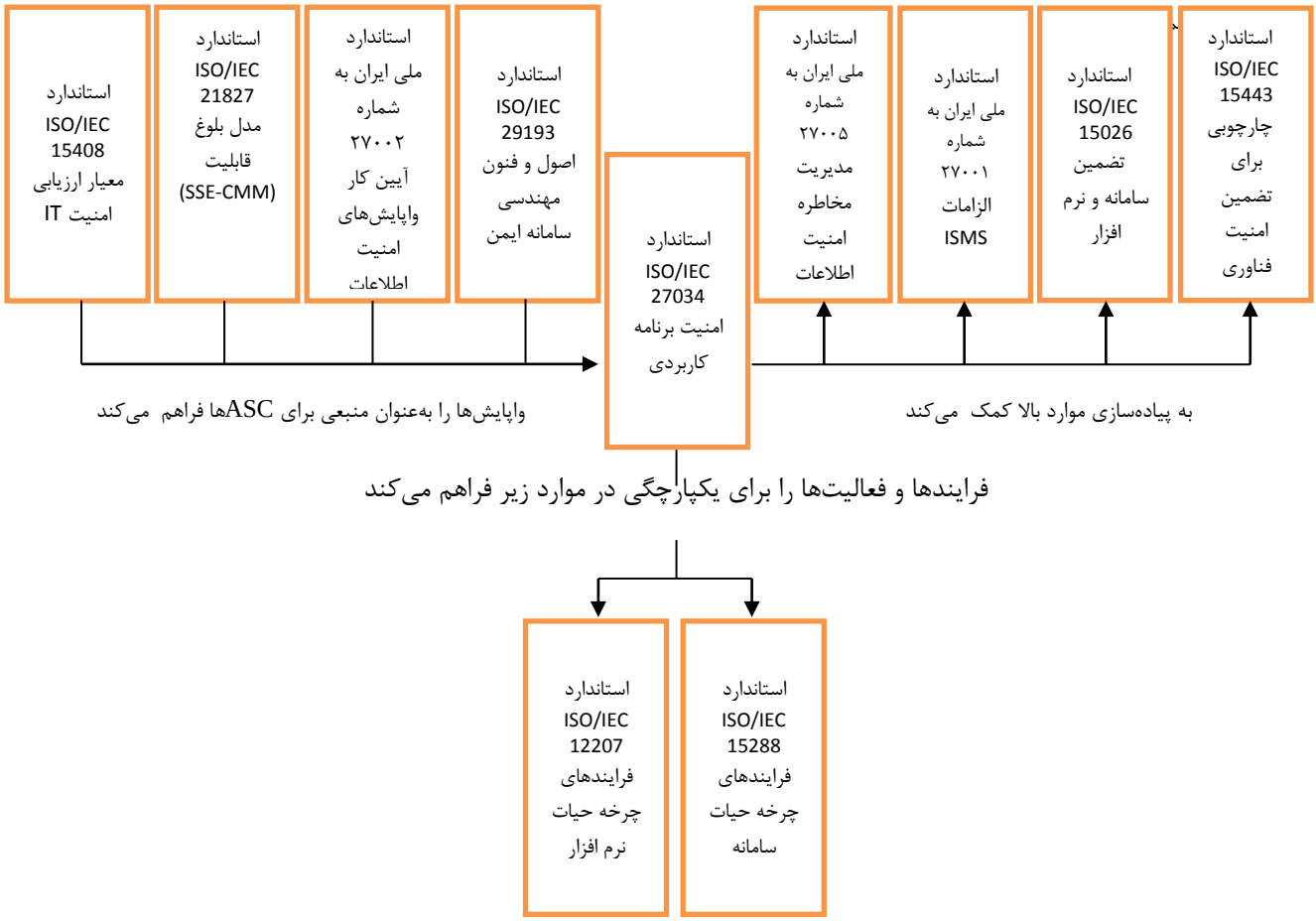
۰-۴-۴ امنیت برنامه کاربردی باید اثبات شود

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

۰-۵ ارتباط با سایر استانداردهای بین‌المللی

۰-۵-۱ کلیات

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



شکل ۱- ارتباط با سایر استانداردهای بین‌المللی

۰-۵-۲ استاندارد ملی ایران به شماره ۲۷۰۰۱ : سال ۱۳۸۷ سامانه‌های مدیریت امنیت اطلاعات- نیازها

استاندارد ISO/IEC 27034 با دامنه‌ای در حد امنیت برنامه کاربردی، به پیاده‌سازی توصیه‌های استاندارد ملی ایران به شماره۲۷۰۰۱ : سال ۱۳۸۷ کمک می‌کند. به‌طور خاص رویکردهای زیر مورداستفاده قرار می-گیرند:

الف- رویکردی نظام‌مند در مدیریت امنیت؛

ب- رویکرد فرایندیِ «برنامه‌ریزی، انجام، بازبینی و عمل»؛ و

پ- پیاده‌سازی امنیت اطلاعات بر پایه مدیریت مخاطره

۰-۵- ۳ استاندارد ملی ایران به شماره ۲۷۰۰۲ : سال ۱۳۸۷ ، فناوری اطلاعات - فنون امنیتی- آیین کار مدیریت امنیت اطلاعات

استاندارد ملی ایران به شماره ۲۷۰۰۲ : سال ۱۳۸۷ تجربه‌هایی را فراهم می‌کند که یک سازمان می‌تواند آن‌ها را همانند واپایش‌های امنیت برنامه کاربردی پیشنهادشده توسط این استاندارد ملی پیاده‌سازی کند. واپایش‌های بندهای زیرین از استاندارد ملی ایران به شماره ۲۷۰۰۲ : سال ۱۳۸۷ مورد بیشترین میزان توجه هستند:

الف- بند ۱۰: مدیریت ارتباطات و عملیات؛

ب- بند ۱۱: واپایش دسترسی؛ و مهم‌تر از همه

پ- بند ۱۲: اکتساب، توسعه و نگهداری سامانه‌های اطلاعاتی.

۰-۵-۴ استاندارد ملی ایران به شماره ۲۷۰۰۵ : سال ۱۳۹۲- مدیریت مخاطرات امنیت اطلاعات

این استاندارد ملی با دامنه‌ای در حد امنیت برنامه کاربردی، به پیاده‌سازی فرایند مدیریت مخاطره پیشنهاد-شده توسط استاندارد ملی ایران به شماره ۲۷۰۰۵ : سال ۱۳۹۲ کمک می‌کند. برای بحث مفصل‌تر به پیوست پ (اطلاعاتی) مراجعه شود.

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

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

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

استاندارد ISO/IEC 15408 نیازها و عناصر کنشگری را که سازمان می‌تواند همانند واپایش‌های امنیت برنامه کاربردی پیشنهادشده توسط این استاندارد ملی پیاده‌سازی کند، فراهم می‌کند.

۰-۵-۷ 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: تحلیل شیوه‌های تضمین

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

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

استفاده از فرایندها و واپایش‌های امنیت برنامه کاربردی این استاندارد ملی در پروژه‌های برنامه کاربردی به‌طور مستقیم موردهای تضمینی راجع به امنیت برنامه کاربردی را تامین می‌کند. به‌طور خاص:

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

ب- شواهد توسط سنجش‌های درستی‌سنجی موجود در واپایش‌های امنیت برنامه کاربردی تامین می‌شوند، و

ج- تطابق با این استاندارد ملی می‌تواند در بسیاری از موردهای تضمینی این‌چنینی به‌عنوان آرگومان استفاده شوند.

همچنین به بند ۸-۱-۲-۶-۵-۱ مراجعه شود.

۰-۵-۹ 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 واپایش‌های امنیت برنامه کاربردی فراهم می‌کند که سازمان می‌تواند به‌عنوان فعالیت‌های افزوده در فرایندهای چرخه حیات مهندسی سامانه‌ها و نرم-افزار موجود همان‌گونه که توسط استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207 فراهم‌شده است، وارد کند.

۰-۵-۱۰ استاندارد ISO/IEC TR 29193 - (درحال‌توسعه)، اصول و فنون مهندسی سامانه امن

استاندارد ISO/IEC TR 29193 ، راهنمایی برای مهندسی سامانه امن سامانه‌هایICT یا محصولاتی که سازمان می‌تواند همانند واپایش‌های امنیت برنامه کاربردی که توسط این استاندارد ملی پیشنهادشده واپایش پیاده‌سازی کند را فراهم می‌کند.

فناوری اطلاعات- فنون امنیتی- امنیت برنامه کاربردی
قسمت ۱: مرور کلی و مفاهیم

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، تعیین راهنمایی برای کمک به سازمان‌ها در یکپارچه‌سازی امنیت در فرایندهای مورداستفاده‌ی مدیریت برنامه‌های کاربردی آن‌ها است.

این استاندارد ملی مروری کلی بر امنیت برنامه کاربردی را ارائه می‌دهد و به تعاریف، مفاهیم، اصول و فرایندهای درگیر در امنیت برنامه کاربردی می‌پردازد.

این استاندارد ملی برای برنامه‌های کاربردی توسعه داده‌شده داخلی، برنامه‌های کاربردی اکتساب‌شده از طرف-های سوم و نیز آنجا که توسعه یا عملیات برنامه کاربردی، برون‌سپاری شده باشد، کاربردپذیر است.

۲ مراجع الزامی

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

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

استفاده از مراجع زیر برای این استاندارد الزامی است:

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

۲-۲ استاندارد ملی ایران به شماره۲۷۰۰۱ :۱۳۸۷، فناوری اطلاعات- فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات- نیازها

۲-۳ استاندارد ملی ایران به شماره ۲۷۰۰۲ : ۱۳۸۷، فن‌آوری اطلاعات - فنون امنیتی -آیین کار مدیریت امنیت اطلاعات

۲-۴ استاندارد ملی ایران به شماره ۲۷۰۰۵ :۱۳۹۲، فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین‌شده در استاندارد ملی ایران به شماره ۲۷۰۰۰ : سال ۱۳۹۱، استاندارد ملی ایران به شماره۲۷۰۰۱ : سال ۱۳۸۷ ، استاندارد ملی ایران به شماره۲۷۰۰۲ : سال ۱۳۸۷ ، استاندارد ملی ایران به شماره ۲۷۰۰۵ : سال ۱۳۹۲، اصطلاحات و تعاریف زیر نیز به کار می‌روند:

۳-۱

کنشگر[1]

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

۳-۲

سطح اعتماد واقعی[2]

نتیجه حاصل از فرایند ممیزی است که دلایل اثبات‌کننده‌ای ارائه می‌کند که همه واپایش‌های امنیتی برنامه کاربردی موردنیاز برای سطح اعتماد هدف‌گذاری شده برنامه کاربردی، به‌طور صحیح پیاده‌سازی و بازبینی‌شده و نتایج موردنظر را ایجاد کرده‌اند.

۳-۳

برنامه کاربردی[3]

راه‌کار فناوری اطلاعات که شامل نرم‌افزار برنامه کاربردی، داده و روال‌های برنامه کاربردی می‌شود و به‌منظور کمک به کاربران یک سازمان برای انجام وظایف خاص یا سامان‌دهی انواع خاص مسائل فناوری اطلاعات با خودکارسازی یک فرایند یا کارکرد کسب‌وکار طراحی‌شده است.

یادآوری- فرایندهای کسب‌وکار افراد و فناوری‌ها را شامل می‌شود.

۳-۴

مدل مرجع چرخه حیات امنیت برنامه کاربردی[4]

مدل چرخه حیات مورداستفاده به‌عنوان مرجع برای معرفی فعالیت‌های امنیتی در فرایندهای درگیر در مدیریت برنامه کاربردی، تامین و عملیات برنامه کاربردی، مدیریت زیرساخت و ممیزی برنامه کاربردی است.

1- Actor
2- Actual Level of Trust
3- Application
4- Application Security Life Cycle Reference Model

۵-۳

چارچوب الزامی برنامه کاربردی(ANF) [1]

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

۶-۳

مالک برنامه کاربردی [2]

نقش سازمانی که مسئول مدیریت، به‌کارگیری و حفاظت از برنامه کاربردی و داده‌های آن است.

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

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

۷-۳

پروژه برنامه کاربردی [3]

تلاشی است با معیارها و ضوابط معین آغاز و پایان که برای اکتساب یک برنامه کاربردی مطابق با منابع و نیازهای خاص، به عهده گرفته می‌شود.

منبع: [استاندارد ISO/IEC 12207 ، تعریف ۴-۲۹، اصلاح‌شده-تخصصی‌شده برای محدوده برنامه کاربردی]

یادآوری- برای اهداف این استاندارد، معیارهای آغاز و پایان به‌گونه‌ای هستند که کل چرخه حیات برنامه کاربردی را در پروژه برنامه کاربردی شامل می‌شوند.

۸-۳

واپایش امنیت برنامه کاربردی (ASC) [4]

ساختمان داده‌ای حاوی شماره‌دهی و توصیف دقیق یک فعالیت امنیتی و سنجش درستی‌سنجی 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 owner
3- Application project
4- Application Security Control

۹-۳

فرایند مدیریت امنیت برنامه کاربردی (ASMP) [1]

کل فرایند مدیریتی برای فعالیت‌ها، کنشگرها، محصولات و ممیزی امنیتی هر برنامه کاربردی کـه مورداسـتفاده یک سازمان قرار می‌گیرد.

۱۰-۳

نرم‌افزار برنامه کاربردی[2]

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

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

۱۱-۳

ممیزی[3]

فرایندی نظام‌مند و مستند شده برای حصول شواهد و ارزیابی عینی آن به‌منظور تعیین گستره‌ی برآورده شدن معیارهای سنجش است.

[منبع: استاندارد ISO/IEC 9000: 2005، تعریف ۳-۹-۱، اصلاح‌شده- تعمیم‌یافته]

۱۲-۳

محیط[4]

زمینه کسب‌وکار، مقرراتی و فناورانه که در آن‌یک برنامه کاربردی مورداستفاده قرارگرفته است. این محیط شامل همه فرایندها، محصولات، اطلاعات و کنشگرهای درگیر در برنامه کاربردی می‌شود.

۱۳-۳

چرخه حیات[5]

سیر تکامل تدریجی یک سامانه، محصول، خدمت، پروژه یا سایر هستارهای ساخته‌ی انسان از آغاز شکل‌گیری تا زمان کنار گذاشته شدن آن است.

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

1- Application Security Management Process
2- Application software
3- Audit
4- Environment
5- Life cycle

۱۴-۳

مدل چرخه حیات[1]

چارچوب فرایندها و فعالیت‌های مرتبط با چرخه حیات که ممکن است به‌صورت چندمرحله‌ای سازمان‌دهی شده باشد. همچنین به‌عنوان مرجعی مشترک برای ارتباطات و ادراکات عمل می‌کند.

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

۱۵-۳

نگهداری[2]

هر تغییری که در یک برنامه کاربردی، پس از تحویل آن انجام شود.

مثال‌ها: تصحیح خطا، کارکرد افزوده، بهبود عملکرد، ایجاد اطمینان از کارکرد برنامه کاربردی.

۱۶-۳

چارچوب الزامی سازمان [3] (ONF)

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

۱۷-۳

کمیته ONF [4]

نقش سازمانی مسئول نگهداری و تصویب مؤلفه‌های مرتبط با امنیت برنامه کاربردی در درون ONF است.

۱۸-۳

محیط بهره‌برداری[5]

محیط بیرونی که وجود دارد یا انتظار می‌رود در طول اجرای یک برنامه کاربردی وجود داشته باشد.

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

۱۹-۳

محصول[6]

نتیجه‌ی یک فرایند است.

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

1- Life cycle model
2- Maintenance
3-Organization Normative Framework
4- ONF committee
5- Operating environment
6- Product

۲۰-۳

برنامه کاربردی امن[1]

برنامه کاربردی که سطح اعتماد واقعی آن برابر با سطح اعتماد هدف‌گذاری شده سازمانی است که برنامه کاربردی را استفاده می‌کند.

۲۱-۳

سطح اعتماد هدف‌گذاری‌شده[2]

نام یا برچسب مجموعه‌ای از واپایش‌های امنیت برنامه کاربردی که توسط مالک برنامه کاربردی به‌منظور کاهش مخاطره‌ی مربوط به یک برنامه کاربردی خاص تا سطح قابل‌قبول (یا قابل‌تحمل)، ضروری فرض شده‌اند، که این سطح اعتماد از یک تحلیل مخاطره امنیت برنامه کاربردی پیروی می‌کند.

۲۲-۳

کاربر[3]

شخصی که از چیزی استفاده می‌کند یا آن را اجرا می‌کند.

[منبع: لغتنامه آکسفورد]

یادآوری- برای اهداف این استاندارد، اصطلاح «کاربر» تنها شامل کاربر نهایی نمی‌شود بلکه شامل نقش‌های عملیاتی و نگهداری از قبیل راهبر سامانه و راهبر دادگان نیز می‌شود.

۲۳-۳

اعتبار سنجی[4]

تأیید برآورده شدن نیازهای یک کاربری یا برنامه‌ی کاربردی خاص موردنظر از طریق ارائه شواهد عینی می باشد.

یادآوری ۱- اصطلاح «اعتبار سنجی شده» برای تعیین وضعیت متناظر به کار می‌رود.

یادآوری ۲- شرایط استفاده برای اعتبارسنجی می‌تواند واقعی یا شبیه‌سازی‌شده باشد.

1- Secure application
2- Targeted Level of Trust
3- User
4- Validation

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

یادآوری ۳- در اصطلاح عامیانه، «اعتبار سنجی» به معنای این است که «آیا برنامه ساخته‌شده همان برنامه کاربردی موردنظر است؟»

۲۴-۳

درستی سنجی[1]

تأیید برآورده شدن نیازهای خاص از طریق ارائه شواهد عینی است.

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

یادآوری ۲- تأیید 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]

یادآوری۳- در اصطلاح عامیانه، «درستی‌سنجی» به این معنا است که «آیا برنامه کاربردی به‌درستی در حال ساخت است؟»

۴ اصطلاحات و کوته‌نوشت‌ها

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

۵ ساختار استاندارد ISO/IEC 27034

استاندارد ISO/IEC 27034 شامل شش قسمت است. این قسمت از استانداردISO/IEC 27034 مرور کلی و مفاهیم ضروری را ارائه می‌کند. این قسمت جامعیت داشته و برای ارزیابی نیاز پیاده‌سازی استاندارد ملی

1- Verification

ISO/IEC 27034 در یک سازمان و نیز برای اهداف نمایش و آموزش کفایت می‌کند. ایـن قسـمت از اسـتاندارد ISO/IEC 27034 به‌تنهایی برای پیاده‌سازی استاندارد ISO/IEC 27034 کافی نیست.

توصیه می‌شود سـازمان‌هایی که تمایل دارند اسـتانـدارد ISO/IEC 27034 را پیاده‌سازی کنند اسـتانـدارهای ISO/IEC 27034-2, 3, 4 باید اکتساب شود. این استانداردها مباحث، شماره دهی‌ها، سـاختارها و توصـیف‌هـای عمیقی برای همه مفاهیم ارائه‌شده در این قسمت از استاندارد ISO/IEC 27034 را شامل می‌شوند.

استاندارد ISO/IEC 27034-5 به‌طور خاص برای سازمان‌هایی مفید خواهد بود که تمایـل دارنـد بـا ایجـاد یـک ساختمان داده‌ی استاندارد و یک پروتکل استاندارد برای توزیع واپایش‌ها، واپایش‌ها را اکتساب کـرده یـا توزیـع کنند. به‌عنوان‌مثال یک سازمان بزرگ ممکن است به توزیع خودکار و نیز بـه‌روزرسـانی واپـایش‌هـا بـرای همـه واحدهای زیرمجموعه خود تمایل داشته باشد.

استاندارد ISO/IEC 27034-6 مثال‌هایی از واپایش‌هایی برای نیازهای خاص امنیت برنامه کاربردی ارائه کرده و برای سازمان‌هایی مفید خواهد بود که تمایل دارند استاندارد ISO/IEC 27034 را پیاده‌سازی کنند یـا سـازمان-هایی که تمایل دارند واپایش‌های 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 مـی‌دهـد. ایـن قسـمت بـه ارائـه تعـاریف، مفـاهیم، اصـول و فرایندهای درگیر در امنیت برنامه کاربردی می‌پردازد.

قسمت ۲- چارچوب الزامی سازمان

قسمت ۲ بحث عمیق در زمینه چارچوب الزامـی سـازمان، مؤلفـه‌هـای آن و فراینـدهای سـطح سـازمانی بـرای مدیریت آن ارائه می‌دهد. این قسمت به توضیح روابط بین این فرایندها، فعالیت‌های مرتبط با آن‌هـا و وسـایل و ابزارهایی می‌پردازد که از طریق آن‌ها این فرایندها از فرایند مدیریت امنیت برنامه کاربردی حمایت می‌کنند. این قسـمت در مـورد این بحث می‌کنـد که توصیه می‌شود چگـونه یـک سـازمان اسـتانـدارد ISO/IEC 27034 را پیاده‌سازی کرده و آن را با فرایندهای موجود خود یکپارچه سازد.

قسمت ۳- فرایند مدیریت امنیت برنامه کاربردی

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

تعیین نیازها و محیط برنامه، ارزیابی مخاطرات امنیت برنامه کاربردی، ایجاد و نگهداری چارچوب الزامـی برنامـه 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 ایـن فرایندها امنیت را در یک پروژه کاربردی ارائه می‌کنند.

قسمت۴- اعتبارسنجی امنیت برنامه کاربردی

قسمت ۴ معرف بحث 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 هدف‌گذاری‌شده برنامـه کـاربردی کـه قـبلاً توسط سازمان انتخاب‌شده، مقایسه می‌کند.

قسمت۵- پروتکل‌ها و ساختمان داده واپایش امنیت برنامه کاربردی

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

قسمت ۶- راهنمای امنیتی برای برنامه‌های کاربردی خاص

قسمت ۶ در صورت لزوم، می‌تواند مثال‌هایی از ASC های واپایش 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 واپایش و سنجش برنامه‌های کاربردی یک سازمان و به‌منظور مدیریت مخاطره‌ی استفاده از آن‌ها، اجرا می‌شود.

واپایش‌ها و سنجش‌ها می‌توانند بر خود برنامه کاربردی (فرایندها، مؤلفه ها، نرم‌افزار و نتایج آن)، داده‌های آن (داده‌های پیکربندی، داده‌های کاربری، داده‌های سازمانی) و نیز بر کل فناوری، فرایندها و کنشگرهای درگیر 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.) بنابراین امنیت برنامه کاربردی مفهومی گسترده‌تر است که امنیت نرم‌افزار را نیز شامل می‌شود.

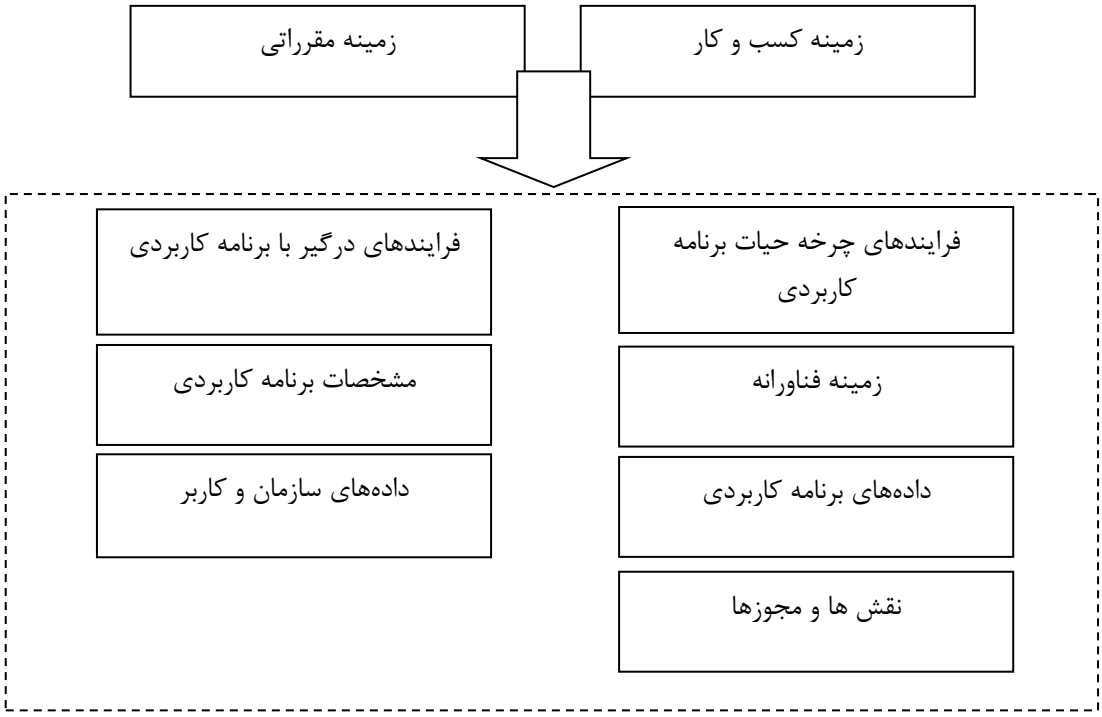
۶-۳ محدوده امنیت برنامه کاربردی

۶-۳-۱ کلیات

امنیت برنامه کاربردی از داده‌های حیاتی که توسط یک برنامه کاربردی متناسب با نیاز سازمان محاسبه، استفاده، ذخیره و منتقل می‌شوند، حفاظت می‌کند. این حفاظت نه‌تنها دسترس‌پذیری، یکپارچگی و محرمانگی داده‌ها را تضمین می‌کند، بلکه احراز هویت و انکارناپذیری کاربرانی که به این اطلاعات دسترسی دارند را تضمین می‌کند. توصیه می‌شود حیاتی بودن داده‌ها و سایر سرمایه‌ها توسط سازمان در فرایند ارزیابی مخاطره امنیتی آن مشخص‌شده باشد.

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

شکل ۲ نمایش ترسیمی محدوده امنیت برنامه کاربردی است. این محدوده در شکل به‌صورت خطچین نشان داده‌شده است.



شکل ۲- محدوده امنیت برنامه کاربردی

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 موردحفاظت 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 (۶-۳-۹)		✓
داده‌های برنامه کاربردی (۶-۳-۸)	✓	✓
نقش‌ها و مجوزها (۶-۳-۱۰)	✓	✓
مشخصات برنامه کاربردی (۶-۳-۷)	✓	✓
زمینه فناورانه (۶-۳-۶)		✓
فرایندهای درگیر در برنامه کاربردی (۶-۳-۵)		✓
فرایندهای چرخه حیات برنامه کاربردی (۶-۳-۴)		✓
زمینه کسب‌وکار (۶-۳-۲)		✓
زمینه مقرراتی (۶-۳-۳)		✓

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

۶-۳-۲ زمینه کسب‌وکار

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

۶-۳-۳ زمینه مقرراتی

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

۶-۳-۴ فرایندهای چرخه حیات برنامه کاربردی

همه فرایندهای سازمانی موجود یا لازم که در چرخه حیات برنامه کاربردی درگیر 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 درگیر با برنامه کاربردی

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

الف- فرایندهای استفاده و مدیریت؛

ب- فرایندهای نگهداری و پشتیبان گیری؛

پ- فرایندهای توزیع و به‌کارگیری؛ و

ت- فرایندهایی که تحت تأثیر برنامه کاربردی قرار می‌گیرند یا موردنیاز آن هستند.

۶-۳-۶ زمینه فناورانه

توصیه می‌شود تمامی مؤلفه‌های فناورانه و محصولاتی که از مشخصات حیاتی یا داده‌های حیاتی حمایت می‌کنند، حفاظت شوند. مانند:

الف- پایانه، شبکه ارتباطی و سایر وسایل جانبی مجاز؛

ب- سامانه عامل، پیکربندی و خدمات؛

پ- پیوندها و درگاه‌های مجاز ارتباطی،

ت- نرم‌افزارهای تجاری آماده و سایر محصولات مانند سامانه‌های مدیریتی دادگان که توسط برنامه و زیرساخت فناورانه آن به کار می‌روند؛

ث- صلاحیت و سایر فرایندهای مرتبط با زمینه فنی؛ و

ج- محصولاتی که تحت تأثیر یا مورداستفاده برنامه کاربردی قرار می‌گیرند.

۶-۳-۷ مشخصات برنامه کاربردی

توصیه می‌شود همه خصوصیات برنامه کاربردی 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 داده‌های برنامه کاربردی

توصیه می‌شود همه اطلاعات برنامه کاربردی حفاظت شوند. مانند:

الف- داده‌های پیکربندی برنامه کاربردی؛

ب- کد دودویی برنامه کاربردی

پ- کد منبع برنامه کاربردی

ت- مؤلفه‌های برنامه‌ای و کتابخانه‌ای ؛ و

ث- مستندات کاربردی اجزا و کارکردهای حیاتی.

۶-۳-۹ داده‌های سازمان و کاربر

توصیه می‌شود همه اطلاعات حیاتی سازمان و کاربر حفاظت شوند. مانند:

الف- گواهی‌ها؛

ب- کلیدهای محرمانه؛

پ- داده‌های حیاتی مرتبط با مأموریت؛

ت-داده‌های شخصی؛ و

ث- داده‌های پیکربندی کاربر.

۶-۳-۱۰ نقش‌ها و مجوزها

توصیه می‌شود همه اطلاعات حیاتی مدیریت هویت و مجوزها مورد حفاظت قرار گیرند. مانند:

الف- داده‌های مدیریت هویت؛

ب- داده‌های شناسایی و اصالت‌سنجی و

پ- داده‌های اختیارات.

۶-۴ نیازهای امنیت برنامه کاربردی

۶-۴-۱ منابع نیازهای امنیت برنامه کاربردی

همان‌طور که در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲ بحث شده است، نیازهای امنیت برنامه کاربردی توسط ارزیابی مخاطره و برطرف سازی مخاطره شناخته می‌شوند و توسط عواملی چون مشخصات

برنامه، محیط هدف‌گذاری شده برنامه (زمینه کسب و کار، مقرراتی و فناورانه) 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 توصیه می‌شود برنامه کاربردی ارائه دهد. این واپایش‌ها باید قبلاً توسط سازمان به‌طور کامل تعیین و تصویب‌شده باشند.

۶-۴-۲ مهندسی نیازهای امنیتی برنامه کاربردی

مهندسی نیازهای برنامه کاربردی فرایند گسترده‌تری بر مبنای گردآوری، تحلیل و تعیین نیازها برای یک برنامه کاربردی است. توصیه می‌شود این فرایند 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، قابل‌فهم و تحلیل‌پذیر است. همچنین نیازها و درنتیجه دست‌یابی باید قابل‌سنجش 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 مورداستفاده قرار دارد. اصطلاح «امنیت اطلاعات» بر اطلاعات به‌عنوان یک سرمایه باارزش که مستلزم حفاظتی مناسب و درخور است، اطلاق می‌شود. بر اساس استاندارد ملی ایران به شماره ۲۷۰۰۰: سال ۱۳۹۱، ISMS مدلی برای برقراری، پیاده‌سازی، بهره-برداری، پایش، بازنگری، نگهداری و اصلاح حفاظت از دارایی‌های اطلاعاتی یک سازمان بر مبنای دیدگاه مخاطره کسب‌وکار را فراهم می‌کند. توصیه می‌شود حفاظت از ارزیابی اطلاعات یک سازمان با مخاطرات مربوطه و سطوح پذیرش کسب‌وکار در یک سطح قرار گیرد.
این مدیریت مخاطرات، بر امنیت اطلاعات تکیه کرده و انواع مخاطرات مربوط به انواع شکل‌های استفاده از اطلاعات توسط 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. توصیه می‌شود امنیت برنامه کاربردی واپایش‌های متناسب و مدارکی فراهم کند تا به مدیران سازمان ثابت کند که مخاطرات موردبحث در به‌کارگیری یک برنامه کاربردی به‌درستی مدیریت‌شده‌اند.
ISMS با تضمین این که همه مخاطرات مربوط به اطلاعات سازمانی ازجمله اطلاعات در دسترس برنامه‌ها، مدیریت‌شده‌اند، بر امنیت برنامه کاربردی حاکم است. واپایش‌های موردنیاز سامانه مدیریت امنیت اطلاعات تا سطح برنامه کاربردی توسعه یافته است.

۶-۵ مخاطره

۶-۵-۱ مخاطره امنیت برنامه کاربردی

مخاطره‌ای که به دنبال استفاده از 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 سوءاستفاده موفقیت‌آمیز تهدیدها از آسیب‌پذیری‌ها.

فعالیت‌های تعیین، پیگیری، ذخیره، سنجش و گزارش مخاطرات برنامه کاربردی بیشترین اهمیت رادارند. نیازهای امنیت برنامه کاربردی و واپایش‌های موردنیاز برای پاسخگویی به آن‌ها یکی از واکنش‌های این مخاطره است. فرایند ارزیابی مخاطره امنیت برنامه کاربردی موردنیاز است زیرا مخاطره در طی زمان تغییر می‌کند و درنتیجه تشخیص و ذخیره مداوم و سازگار اطلاعات مخاطره موردنیاز است.

۶-۵-۲ آسیب‌پذیری‌های برنامه کاربردی

آسیب‌پذیری‌ها نتیجه واپایش‌های ناکافی یا ناموجود هستند. آسیب‌پذیری‌هایی که نتیجه واپایش نامناسب هستند منجر به مخاطره غیرقابل‌قبول برنامه کاربردی می‌شوند.

آسیب‌پذیری‌ها ناشی از موارد زیر هستند:

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

ب- فرایندهایی مانند رویه‌ای نامناسب آزمایش، مدیریت ضعیف پروژه، تمرکز ناکافی بر امنیت در کل فرایندهای چرخه حیات، اثرات متقابل پیش بینی‌نشده بین برنامه‌های کاربری، کاربران و اپراتورها، فرایندهای نامناسب مدیریت تغییرات؛

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

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

۶-۵-۳ تهدیدهای برنامه‌های کاربردی

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

الف- محیط برنامه کاربردی: زمینه مقرراتی، زمینه کسب‌وکار و زمینه فناورانه؛ و

ب- کنشگران.

۶-۵-۴ تأثیر بر روی برنامه‌های کاربردی

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

۶-۵-۵ مدیریت مخاطره

مدیریت مخاطره امنیت برنامه کاربردی، فرایند حفظ مخاطرات امنیت برنامه کاربردی در محدوده سطوح قابل‌قبول است. این مدیریت از طریق برطرف سازی مخاطرات غیرقابل‌قبول امنیت برنامه و به‌ویژه از طریق اعمال واپایش بر این مخاطرات حاصل‌شده است.

مدیریت مخاطره یک مفهوم کلیدی در امنیت اطلاعات است. بر اساس استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲، «فرایند مدیریت مخاطره امنیت اطلاعات می‌تواند برای سازمان به‌عنوان یک کلیت، یا برای هر قسمت مجزای سازمان (مانند یک دپارتمان، یک مکان فیزیکی، یک خدمت)، یا برای هر سامانه اطلاعاتی موجود یا طراحی‌شده یا ابعاد خاصی از واپایش (مانند طرح‌ریزی مداوم کسب‌وکار) به کار رود.»

فرایند مدیریت مخاطره امنیت اطلاعات که در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲،ارائه‌شده مبتنی بر استقرار زمینه، ارزیابی مخاطره، برطرف سازی مخاطره، پذیرش مخاطره، اطلاع‌رسانی مخاطره، پایش و بازنگری مخاطره است.

توصیه می‌شود یک فرایند مدیریت مخاطره امنیت برنامه کاربردی از عناصر فرایندی مشابه با اجزای ظریف‌تر و هدفی سازگار با سطح برنامه کاربردی استفاده کند.

۶-۶ هزینه‌های امنیت

توصیه می‌شود هزینه اجرا، نگهداری و درستی سنجی واپایش‌های امنیتی برای یک سازمان بعد از بررسی مناسب مخاطرات و اثرات مرتبط با به‌کارگیری یک برنامه کاربردی، تا یک سطح قابل‌قبول (یا قابل‌تحمل) کاهش یابد. هزینه امنیت باید فشار بالقوه تهدیدات و آسیب‌پذیری‌ها را موردمحاسبه قرار دهد.

۶-۷ محیط هدف

محیط هدف شامل زمینه مقرراتی، کسب‌وکاری و فنی است که سازمان در درون آن از برنامه کاربردی استفاده می‌کند. همه تهدیداتی که ممکن است به برنامه کاربردی آسیب بزنند ناشی از محیط آن هستند. به این دلیل، توصیه می‌شود محیط هدف برنامه کاربردی به‌طور واضح در آغاز یک پروژه برنامه کاربردی تعریف‌شده باشد.

توصیه می‌شود به‌منظور توسعه موفق و امن برنامه کاربردی، زمینه فنی سازمان با نیازهای محیط هدف برنامه موافقت کند. به‌محض این‌که برنامه کاربردی پیاده‌سازی شد، زمینه فنی سازمان می‌بایست محصولات و سخت-افزار جدیدی را اضافه کند که بتوانند بر امنیت سایر برنامه‌های کاربردی اثر گذاشته و مخاطرات امنیت سازمان را تحت تأثیر قرار دهند.

ازآنجاکه مخاطره استفاده از برنامه کاربردی برای سازمان به محیط هدف برنامه مربوط می‌شود، توصیه می‌شود نیازهای امنیتی جدید برنامه کاربردی به‌گونه‌ای تعریف شوند که این مخاطره‌های جدید را مدنظر قرار داده و واپایش‌هایی را انتخاب کنند که این‌گونه مخاطره‌ها را به حد قابل‌قبول (یا قابل‌تحمل) کاهش می‌دهند. چنین واپایش‌های امنیتی را می‌توان وارد فرایندهای چرخه حیات برنامه کاربردی کرد (مانند فرایند اکتساب یا فرایند امحا)، به کد منبع برنامه اضافه کرد یا بنا به نیاز سازمان درجایی از چرخه حیات برنامه کاربردی (بند ۸-۳-۴) ادغام کرد.

۶-۸ واپایش‌ها و اهداف آن‌ها

همان‌گونه که در استاندارد ملی ایران به شماره۲۷۰۰۱ : **سال** ۱۳۸۷تعیین‌شده است، توصیه می‌شود واپایش‌ها و اهداف آن‌ها جهت تامین نیازهایی انتخاب و پیاده‌سازی شوند که توسط فرایندهای ارزیابی مخاطره و مقابله با مخاطره تعیین می‌شوند. در مبحث امنیت برنامه کاربردی، فرایند ارزیابی مخاطره، اهداف واپایش را بر اساس نیازهای امنیتی تعریف‌شده برنامه کاربردی تعیین می‌کند.

۷ فرایندهای کلی این استاندارد ملی

۷-۱ مؤلفه‌ها، فرایندها و چارچوب‌ها

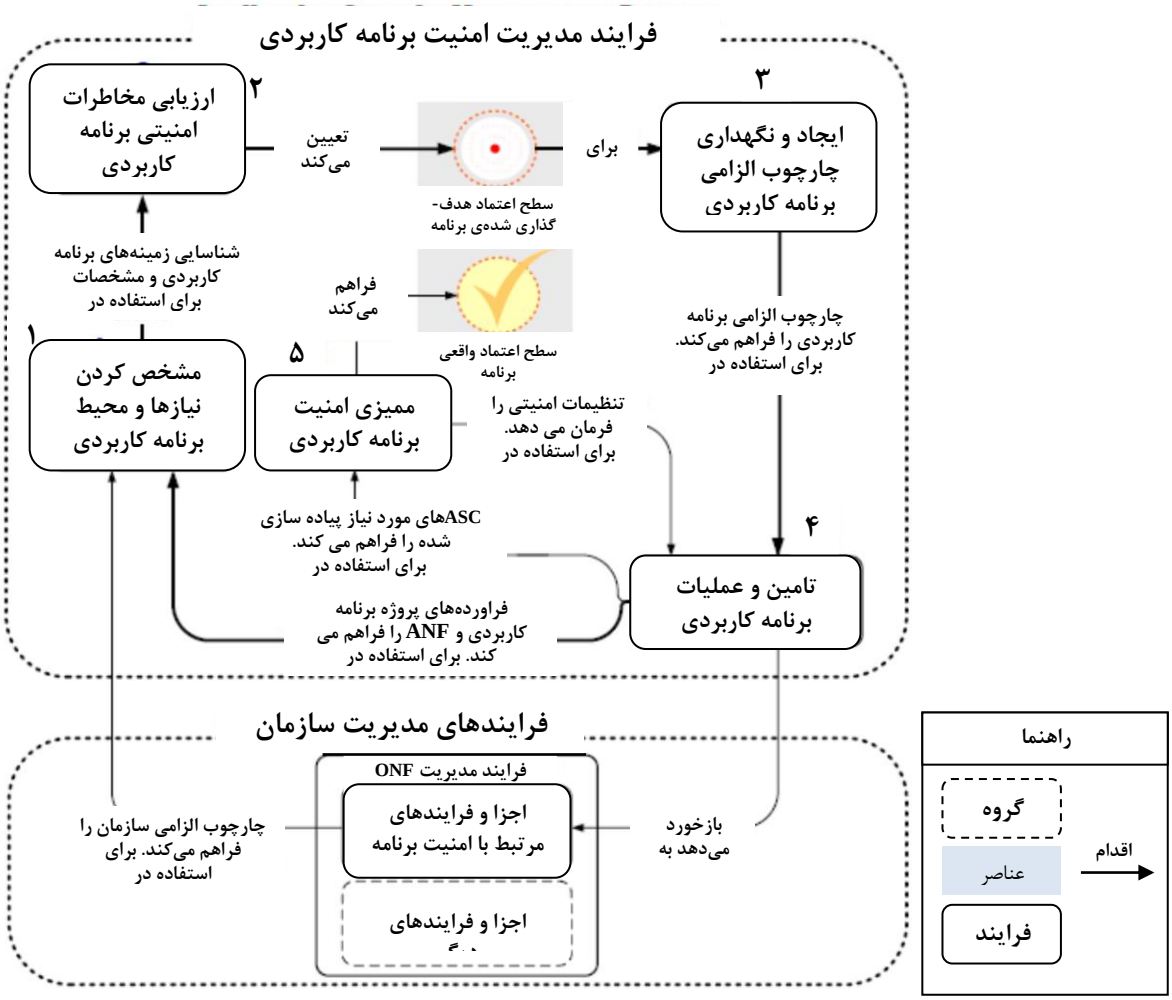
این استاندارد ملی مؤلفه‌ها، فرایندها و چارچوبی برای کمک به سازمان‌ها جهت اکتساب، اجرا و استفاده از برنامه‌های کاربردی قابل‌اطمینان و با زیان امنیتی قابل‌قبول (یا قابل‌تحمل)، ارائه می‌کند. به‌طور خاص‌تر، این مؤلفه‌ها، فرایندها و چارچوب‌ها از این‌که برنامه‌های کاربردی به سطح موردنظر از اطمینان رسیده و در همان سطح باقی‌مانده‌اند شواهد قابل درستی‌سنجی را ارائه می‌کند.

تمام مؤلفه‌ها، فرایندها و چارچوب‌ها قسمتی از دو فرایند کلی هستند که در شکل ۳ نیز نمایش داده‌شده‌اند:

الف- فرایند مدیریت ONF

ب- فرایند مدیریت امنیت برنامه کاربردی ASMP

این دو در سطح و بازه‌های زمانی متفاوتی در سازمان مورداستفاده قرارگرفته و محدوده‌های متفاوتی نیز دارند. «فرایند مدیریت ONF» فرایندی مستمر در سطح سازمان است و «ASMP» جهت مدیریت امنیت در پروژه برنامه‌های کاربردی خاص استفاده می‌شود.



شکل۳ - فرایندهای مدیریت سازمان

۷-۲ فرایند مدیریت ONF

این فرایند باید جهت مدیریت جنبه‌هایی از ONF (چارچوب الزامی سازمان، به بند ۸-۱ مراجعه شود.) استفاده شوند که **مرتبط با امنیت برنامه کاربردی** است. این چارچوب شامل کلیه فرایندهای درگیر در امنیت برنامه کاربردی و همچنین مقررات، قوانین، به‌روش‌ها، نقش‌ها و مسئولیت‌های موردقبول سازمان است. این فرایند تمامی زمینه‌های سازمان را تعریف کرده و مرجع منحصربه‌فرد امنیت برنامه کاربردی درون سازمان می‌شود.

یادآوری۱- سازمان معمولاً چارچوب الزامی را جهت اهداف دیگری خارج از دامنه این استاندارد ملی به کار می‌گیرد و معمولاً فرایندهایی نیز به‌منظور مدیریت آن تعریف می‌کند. بنابراین **ONF** و فرایندهای مدیریتی مربوط به آن از دیدگاه تامین اهداف این استاندارد ملی، زیرمجموعه‌ای از یک **ONF** موجود و فرایندهای مربوطه است.

فرایندهای مرتبط با امنیت برنامه کاربردی باید قسمتی از ONF باشند.

بر اساس 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 «کمیته ONF» می‌نامند.

یادآوری۲- فرایند مدیریت **ONF** و مؤلفه‌های مربوطه و فرایندهای زیرمجموعه با جزئیات بیشتر در بند 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 مورداستفاده یک سازمان است. پیوست پ نشان می‌دهد که ASMP نمونه تخصصی‌شده فرایند مدیریت مخاطره استاندارد استاندارد ملی ایران به شماره۲۷۰۰۱ : سال ۱۳۸۷ 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

پ- ایجاد و نگهداری چارچوب الزامی برنامه کاربردی

ت- تامین و عملیات برنامه کاربردی

ث- ممیزی امنیت برنامه کاربردی

یادآوری- **ASMP** به‌تفصیل دربند ۸ و در استاندارد **ISO/IEC 27034-3** آمده است.

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

مرحله 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 فناورانه

ب- زمینه کسب‌وکار

پ- زمینه مقرراتی

یادآوری- زمینه به‌تفصیل در بندهای ۸-۱-۲-۱ و ۸-۱-۲-۲ ارائه‌شده است.

این مرحله مربوط به مرحله تأسیس زمینه در فرایند مدیریت مخاطره می‌شود که توسط استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲، تعیین‌شده و اطلاعات لازم جهت مرحله بعدی ارزیابی مخاطره را فراهم می‌کند.

۷-۳-۳ ارزیابی مخاطرات امنیت برنامه کاربردی

مرحله دوم ASMP فرایندی مطابق با «ارزیابی مخاطره» و قسمتی از مرحله «برطرف سازی مخاطره» در فرایند مدیریت مخاطره‌ای است که در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲ 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 اکتساب سطح اعتماد مطلوب یک برنامه کاربردی مورداستفاده قرار می‌گیرند. این موضوع سطح اعتماد هدف‌گذاری‌شده نام دارد و باید مورد تأیید مالک برنامه کاربردی قرار گیرد.

به همین دلیل این مرحله با قسمت «انتخاب روش برطرف سازی مخاطره » از مرحله «برطرف سازی مخاطره» در فرایند مدیریت مخاطره در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲ مطابقت دارد.

۷-۳-۴ ایجاد و نگهداری چارچوب الزامی برنامه

مرحله سوم ASMP، تمام عناصر مرتبط ONF قابل‌اعمال بر یک پروژه کاربردی خاص را انتخاب می‌کند. نتیجه آن چارچوب الزامی برنامه کاربردی (ANF) خواهد بود. سطح اعتماد هدف‌گذاری شده برنامه کاربردی، زمینه-های برنامه کاربردی (مقرراتی، کسب وکار یا فناورانه)، مسئولیت‌ها 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 موردنیاز پروژه حاضر را تعیین می‌کند. به‌عنوان‌مثال یک پروژه درون‌سازمانی نیاز به فعالیت‌های برون‌سپاری ندارد.

درمجموع، سازمان واپایش‌های امنیت برنامه کاربردی قابل‌اجرا برای پروژه برنامه کاربردی را انتخاب می‌کند.

این مرحله مطابق قسمت «آماده‌سازی و پیاده‌سازی برنامه‌های برطرف سازی مخاطره» است که خود قسمتی از مرحله «برطرف سازی مخاطره» در فرایند مدیریت مخاطره تعیین‌شده در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲است.

یادآوری- این مرحله از **ASMP** و مؤلفه‌ها و فرایندهای مربوطه با جزئیات بیشتر در بند ۸-۳ ارائه‌شده است.

۷-۳-۵ تامین و عملیات برنامه کاربردی

مرحله چهارم ASMP استفاده واقعی از «واپایش‌های امنیتی برنامه کاربردی»، مطابق آنچه توسط ANF در چرخه حیات برنامه کاربردی ارائه شده است. گروه پروژه، واپایش‌های امنیت برنامه کاربردی را تحت چارچوب الزامی سازمان، در دو مرحله فرعی 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 برطرف سازی مخاطره» است که خود قسمتی از مرحله «برطرف سازی مخاطره» در فرایند مدیریت مخاطره تعیین‌شده استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲است.

یادآوری- این مرحله از **ASMP** و مؤلفه‌ها و فرایندهای مربوط با جزئیات بیشتر در بند ۸-۴ ارائه‌شده 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 ارائه‌شده توسط ASCها در چارچوب الزامی برنامه کاربردی و دست‌یابی به نتایج موردنظر را می‌سنجد.

این مرحله مطابق مرحله «پایش و بازبینی» فرایند مدیریت مخاطره تعیین‌شده در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲ است.

یادآوری- این مرحله از **ASMP** و اجرا و فرایندهای مربوط با جزئیات بیشتر در بند ۸-۵ ارائه‌شده است.

۸ مفاهیم

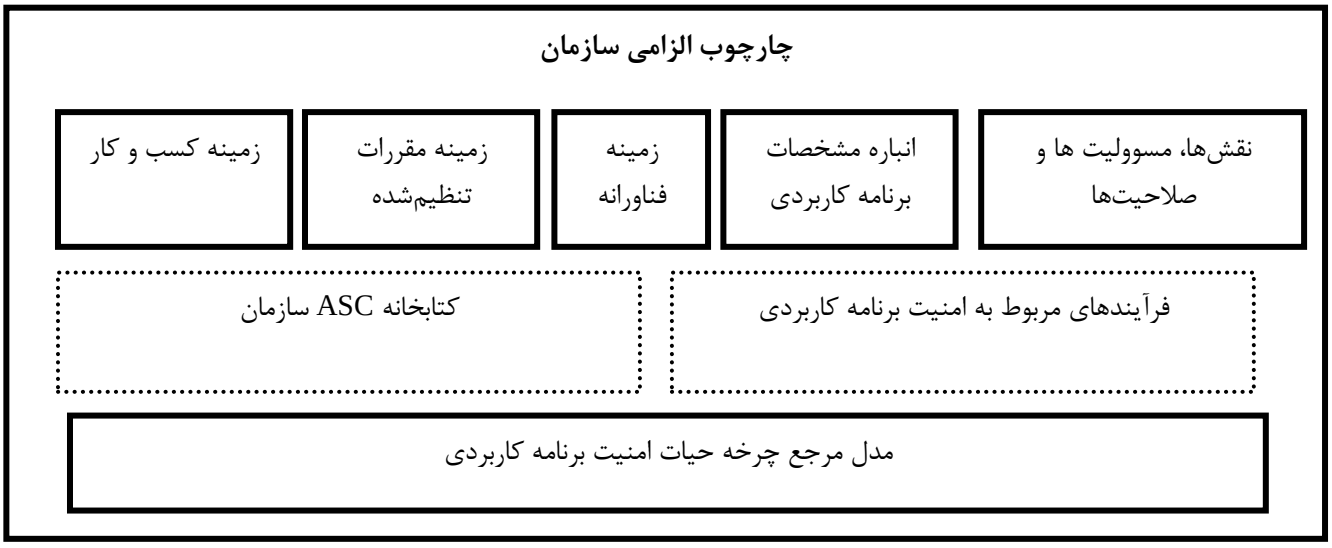
۸-۱ چارچوب الزامی سازمان

۸-۱-۱ کلیات

چارچوب الزامی سازمان (ONF) چارچوبی است که در آن بهترین روش‌های امنیت برنامه کاربردی ازنظر سازمان مربوطه ذخیره‌شده یا بهترین روش‌های امنیت برنامه از آن بازیافت یا استخراج می‌شوند. این چارچوب مؤلفه‌های ضروری، فرایندهایی که این مؤلفه‌ها را مورداستفاده 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 بر اساس آن اتخاذ می‌شوند. به‌عنوان‌مثال، اگر راهنماهای کدگذاری در ONF موجود باشند، فعالیت بازنگری کد به‌عنوان واپایش 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 سطح بالا از محتویات ONF را نمایش می‌دهد.



شکل ۴- چارچوب الزامی سازمان (ساده‌شده)

به‌منظور پرداختن صحیح به نگرانی‌های امنیت برنامه کاربردی، توصیه می‌شود یک سازمان ONF رسمی شامل مؤلفه‌های زیر را داشته باشد:

الف- زمینه کسب‌وکار

ب- زمینه مقرراتی

پ- زمینه‌های فناورانه

ت- انباره مشخصات برنامه کاربردی

ث- نقش‌ها، مسئولیت‌ها و صلاحیت‌ها

ج- کتابخانه ASC سازمان

چ- فرایندهای مربوط به امنیت برنامه کاربردی

ح- مدل مرجع چرخه حیات امنیت برنامه کاربردی

ONF رسمی باید شامل فرایندهای زیر نیز باشد:

الف- فرایند مدیریت ONF

ب- زیر فرایندهای مدیریت ONF

۸-۱-۲ مؤلفه‌ها

۸-۱-۲-۱ زمینه کسب‌وکار

زمینه کسب‌وکار تمام استانداردها و بهترین روش‌های به کار گرفته‌شده توسط سازمان را که می‌توانند بر پروژه-های کاربردی تأثیرگذار باشند را فهرست و ثبت می‌کند.

زمینه کسب‌وکار شامل موارد زیر می‌شود:

الف- فرایندهای مدیریت پروژه، توسعه، تحلیل مخاطره، عملیات، ممیزی و واپایش

ب- خط‌مشی امنیتی سازمان

پ- روش‌های زمینه کسب‌وکار

ت- روشگان[1] توسعه استفاده‌شده توسط سازمان

ث- بهترین روش‌ها در مورد کلیه زبان‌های برنامه‌نویسی استفاده‌شده توسط سازمان و فهرست شده در زمینه فناورانه.

ج- فرایند مدیریت پروژه رسمی سازمان

چ- اقتباس سایر استانداردهای ISO/IEC مرتبط مانند استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، استاندارد ملی ایران به شماره ۲۷۰۰۲: سال ۱۳۸۷ و استاندارد ISO/IEC 5288 .

1- Methodology

۸-۱-۲-۲ زمینه مقرراتی

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، نیازهای کارکرد عمومی فناوری اطلاعات سازمان را همراه با راه‌حل‌های از پیش تعیین‌شده 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 نیازهای معمول برنامه کاربردی

پ- کد منبع، کد دودویی، 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 واپایش‌های موجود در محیط زمان اجرای برنامه کاربردی

۸-۱-۲-۴ زمینه فناورانه

زمینه فناورانه از انباره کلیه محصولات، خدمات و فناوری‌های فناوری اطلاعات تشکیل‌شده 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 فناورانه شامل رایانه‌ها، ابزارها، محصولات و خدمات فناوری اطلاعات، زیرساخت ارتباطات و سایر وسایل فنی است.

مثال۱: زمینه‌های فناورانه که ممکن است تأثیری بر امنیت برنامه کاربردی داشته باشند، زیرساخت سرویس‌دهنده/مشتری، زیر-ساخت وب، زیرساخت شبکه، محیط و ابزارهای توسعه را شامل می‌شوند.

زمینه فناورانه همچنین امکان معرفی واپایش‌های امنیت برنامه کاربردی خاص را در برنامه کاربردی مشخص می‌کند.

مثال ۲: اگر زمینه فناورانه شامل سازوکار احراز هویت TLS1.0 جهت پشتیبانی از کارکرد احراز هویت دوسویه نباشد، ممکن است برنامه کاربردی شامل ASC مبتنی بر TLS.1.0 نباشد. اگر این کارکرد در سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی موردنیاز باشد، گروه پروژه بایدASC جایگزینی را برای دست‌یابی به کارکرد احراز هویت دوسویه انتخاب کند.

توصیه می‌شود زمینه فناورانه شامل موارد زیر باشد:

الف- فناوری‌های در دسترس جهت پروژه‌های برنامه کاربردی سازمان

توصیه می‌شود این انبار فناوری به‌صورت مداوم توسط کمیته ONF سازمان و از طریق بازخورد پروژه‌های برنامه کاربردی پیشین به‌روزرسانی شود.

ب- فناوری‌های موردنیاز برنامه کاربردی؛

فهرست فناوری‌های جدید از نیازهای کارکردی جدید مشخص‌شده در جریان برنامه‌ریزی تشویقی پروژه برنامه کاربردی سرچشمه می‌گیرند. توصیه می‌شود چنین نیازهایی به ONF اضافه شوند و یک فرایند سازمانی می‌بایست از این امر اطمینان حاصل کند که خصوصیات امنیتی فناوری‌های خاص جهت برآوردن نیازهای جدید، قبل از تأیید، جهت قرار گرفتن در انبار فناوری‌های سازمان درک و ثبت‌شده‌اند؛ و

پ- فناوری‌های در دسترس؛

این مورد حاصل تحقیق، تحلیل روند و پایش فناوری است.

۸-۱-۲-۵ نقش‌ها، مسئولیت‌ها و صلاحیت‌ها

توصیه می‌شود **ONF** شامل موارد زیر باشد:

الف- فهرست‌ها و توصیف تمام نقش‌ها، مسئولیت‌ها و صلاحیت‌ها و صلاحیت‌های حرفه‌ای موردنیاز کنشگرهای درگیر در ایجاد و نگهداری و/یا نقش‌های ایجاد و نگهداری ASCها؛ و

ب- - فهرست‌ها و توصیف تمام نقش‌ها، مسئولیت‌ها و صلاحیت‌ها و صلاحیت‌های حرفه‌ای موردنیاز کنشگرهای درگیر در چرخه حیات برنامه کاربردی سازمان ازجمله: مدیران امنیت اطلاعات، مدیران پروژه، راهبران، به‌دست-آورنده‌های نرم‌افزار، مدیران توسعه نرم‌افزار، مالکان برنامه کاربردی، مدیران کاربری، مهندسین معمار، تحلیل-گران، برنامه‌نویسان، آزماینده‌ها، راهبران سامانه، راهبران دادگان‌ها، راهبران شبکه و کارکنان فنی.

این‌یک خط‌مشی جامع سازمانی است که کمک می‌کند تا اطمینان حاصل شود تمام نقش‌های حیاتی فرایندها پرشده‌اند، تمام مسئولیت‌ها تعریف‌شده‌اند، از تضاد منافع جلوگیری شده است و تمام افرادی که نقش‌ها را پر-کرده‌اند صلاحیت‌های حرفه‌ای کافی را دارند.

۸-۱-۲-۶ کتابخانه ASC سازمان

۸-۱-۲-۶-۱ کلیات

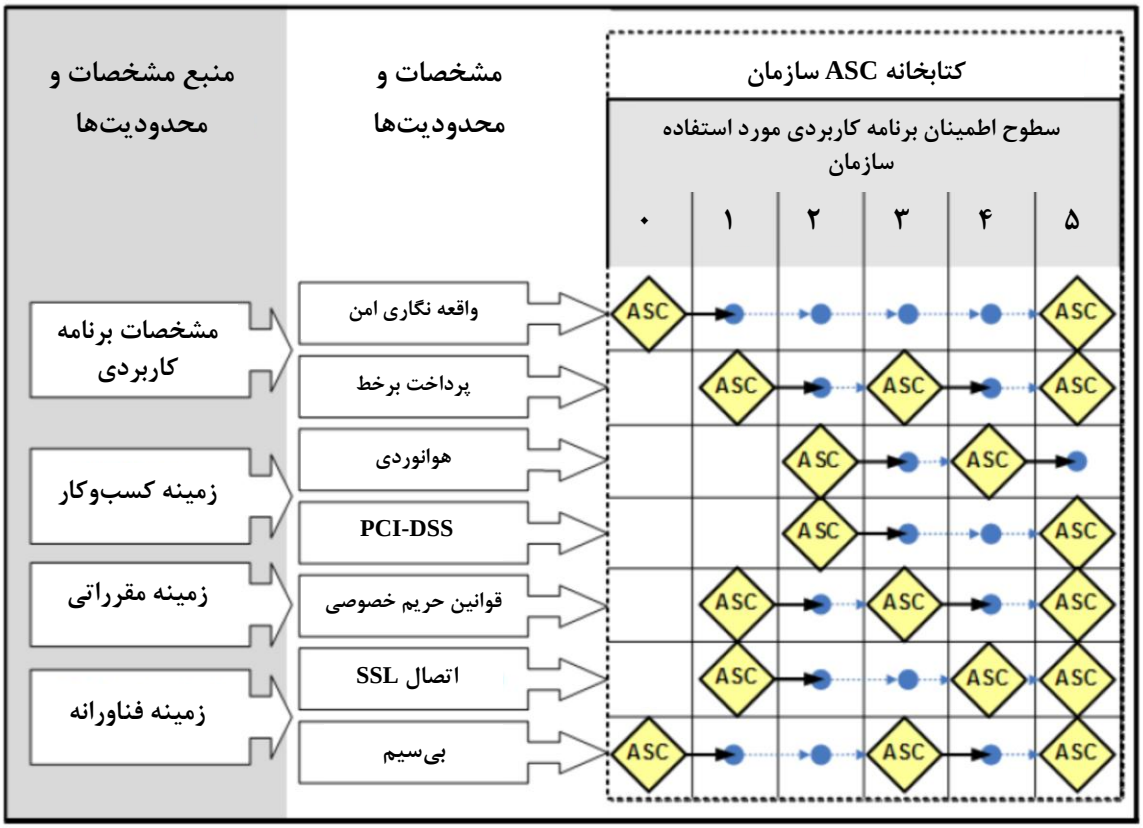
توصیه می‌شود سازمان کمینه یک کتابخانه از واپایش‌های امنیت برنامه کاربردی تعریف کند. این کتابخانه، کتابخانه واپایشی امنیت برنامه کاربردی (کتابخانه ASC) نامیده می‌شود. این کتابخانه تمام ASCهای شناخته-شده در سازمان را فهرست و ثبت می‌کند. این ASCها از استانداردها، به‌روش‌ها و نقش‌ها، مسئولیت‌ها، نقش‌ها، صلاحیت‌های حرفه‌ای، زمینه‌های فنی، کسب‌وکاری و مقرراتی و مشخصات برنامه کاربردی استنتاج شده‌اند.

واپایش‌های امنیت برنامه کاربردی موجود در این کتابخانه در مجموعه‌هایی بر اساس 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 اکتساب‌شده از مجموعه واپایش‌های تعریف‌شده‌ی مشخص آگاه سازد. اگر برای مجموعه‌ای از واپایش‌ها سطح پایینی از اطمینان توصیف شده باشد، آن مجموعه حفاظت محدودی از امنیت اطلاعات فراهم می‌کند. اگر برای مجموعه‌ای از واپایش‌ها سطح بالایی از اطمینان توصیف‌شده باشد، آن مجموعه سطح بالایی از حفاظت را فراهم می‌کند. سطوح اعتماد بیشتر در بند ۸-۱-۲-۶-۴ توصیف‌شده‌اند.

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 ASCسازمانی موجود را نشان می‌دهد. سازمان این مثال برنامه‌های کاربردی را در زمینه هوانوردی توسعه می‌دهد. کتابخانه حاوی تمام واپایش‌های موردنیاز سازمان برای پیاده‌سازی کارکردها، به‌روش‌ها، استانداردها و قوانین و مقررات قابل کاربرد است.



شکل ۵- نمایش گرافیکی مثالی از کتابخانه ASC سازمان

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

این مثال ساده نشان می‌دهد که مشخصات برنامه کاربردی سازمان و همچنین زمینه کسب‌وکار، مقرراتی و فنی آن، محتویات کتابخانه ASC یک سازمان را مشخص می‌کند. به‌این‌ترتیب کتابخانه ASC هر سازمان مختص آن سازمان خاص خواهد بود.

۸-۱-۲-۶-۳ فرایند ایجاد کتابخانه ASC سازمان

فرایند ایجاد کتابخانه ASC سازمان ساده است و حتی برای کوچک‌ترین سازمان‌ها به‌راحتی قابل‌اجرا است.

کتابخانه در ابتدا خالی است. ASCها با گروه‌بندی در ستون‌هایی که مطابق سطح اعتماد آن‌ها است (به ستون-های 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 نیازهای سازمان را تامین کند.
با تحلیل برنامه‌های کاربردی موجود یا جدید سازمان، به بهترین شکل به مقصود می‌رسیم. این تحلیل مشخص کردن مخاطره‌ها و نیازهای امنیتی برای برنامه کاربردی است و سپس انتخاب یا ایجاد ASCهای درخور آن نیازها را دربر می‌گیرد. برای هر برنامه کاربردی که تحلیل می‌شود نتیجه، مجموعه‌ای از ASCها است.
این مجموعه از ASCها می‌تواند از سه‌راه با کتابخانه ASC موجود تطابق داشته باشد:
الف- تمام مجموعه ASCها از قبل شامل سطح اعتماد کتابخانه است که در این صورت هیچ‌چیز به کتابخانه اضافه نمی‌شود.
ب- یکی از سطوح اعتماد موجود با مجموعه کامل ASCها تطابق نزدیکی دارد که در این صورت کتابخانه با ASCهای مجموعه می‌تواند کامل شود.
پ- سطح اعتماد جدیدی از مجموعه ASCها در کتابخانه ایجاد می‌شود.
بنابراین ممکن است سازمانی تصمیم بگیرد یا از تخصص‌های موجود و از طریق استفاده مجدد از واپایش‌های امنیتی برنامه‌های کاربردی موجود واپایش‌ها را بسازد یا واپایش‌های جدیدی تولید کرده یا به دست آورد، یا هر دو روش را به کار گیرد.

کتابخانه ASC سازمان در پاسخ به بازخورد هر پروژه برنامه کاربردی جدید همان‌طور که در بند ۸-۱-۳-۲ مطرح‌شده 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 واپایش‌ها 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 داده‌شده 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 تعریف‌شده‌اند، همان‌طور که با فلش‌هایی که به نقطه‌ها ختم می‌شوند نشان داده‌شده‌اند، در سطح ۱ نیز به کارمی روند.

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

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

توصیه می‌شود سازمان 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 بر پایه معیار پذیرش مخاطره استفاده کند.

توصیه می‌شود سازمان سطح اعتماد قابل‌پذیرش کمینهی را برای هر یک از برنامه‌های کاربردی خود تعریف کند. این استاندارد ملی برای تعریف سطح اعتماد قابل‌پذیرش کمینه (در مقابل سطح اعتماد قابل‌پذیرش بیشینه) 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 قرار گرفت، 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 هدف‌گذاری‌شده‌ی برنامه کاربردی مشخص با تحلیل مخاطره این برنامه کاربردی، سطح اعتماد صفر باشد، این ASC همچنان باید اجرا شود.

۸-۱-۲-۶-۵ واپایش امنیت برنامه کاربردی

۸-۱-۲-۶-۵-۱ کلیات

واپایش 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 موردنیاز برای تأیید برنامه کاربردی موفق را بیان می‌کند.

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

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

برای سازمان‌هایی که مفهوم حصول اطمینان را همان‌گونه که در استاندارد ملی ایران به شماره ۱۵۰۲۶-۲تعریف‌شده، پیاده‌سازی کرده‌اند، ASCها برای مدیریت آسان و فراهم آوردن به‌موقع شواهد موردنیاز برای

پشتیبانی ادعاها و استدلال‌های مربوط به امنیت یک برنامه کاربردی مفید هستند. پشتیبانی بیشتر از استدلال‌ها با به‌کارگیری مداوم فرایندهای پیشنهادی این IS برای ایجاد، تأیید و استفاده از هر ASC تامین می‌شود. ازآنجایی‌که کل مجموعه ASCهای انتخاب‌شده برای پروژه برنامه کاربردی از تحلیل مخاطره امنیت برنامه کاربردی سرچشمه می‌گیرند، این مجموعه به‌طور مستقیم ادعاهای سطح بالایی، توجیهات و استدلال‌های مربوط به امنیت برنامه کاربردی را پشتیبانی می‌کند.

ASCها می‌توانند در موارد زیر مورداستفاده قرار گیرند:

الف- امن‌سازی مؤلفه‌های برنامه کاربردی ازجمله نرم‌افزار، داده، نرم‌افزارهای تجاری و عمومی و زیرساخت

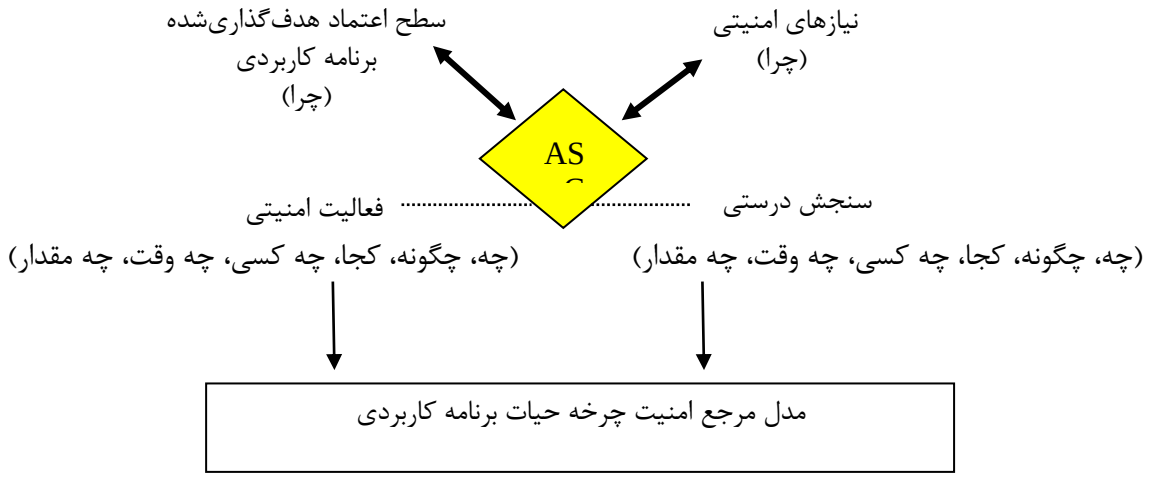
ب- افزودن فعالیت‌های امنیتی به فرایندهایی که در مراحل چرخه حیات برنامه کاربردی استفاده می‌شوند.

پ- تأیید نقش‌ها، مسئولیت‌ها و صلاحیت‌های حرفه‌ای کلیه کنشگرهای درگیر در یک پروژه

ت- تعیین معیار ارزیابی/پذیرش مؤلفه‌ها

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 اجراشده است.) فراهم می‌آورد.



شکل ۶ – مؤلفه‌های یک ASC

قسمت فعالیت ASC چگونگی برخورد با مسائل امنیتی یک پروژه برنامه کاربردی را مشخص می‌کند.

قسمت سنجش ASC چگونگی تامین شواهد دال بر این‌که فعالیت به‌درستی، توسط کنشگری باصلاحیت انجام‌شده است و نتایج مورد انتظار فراهم‌شده است را مشخص می‌کند.

فعالیت و سنجش، هر دو هزینه تخمینی را فراهم می‌کنند که به سازمان در ارزیابی و تأیید هزینه‌های کلی واپایش‌های امنیت مربوط به سطح اعتماد هدف‌گذاری‌شده، کمک می‌کند.

ASCها می‌توانند در یک نمودار به هم متصل شوند به‌این‌ترتیب می‌توان فعالیت را پس از اجراشدن در ASC توسط فعالیت‌های خرد ادامه داد. این ویژگی ASC در موارد زیر مفید است:

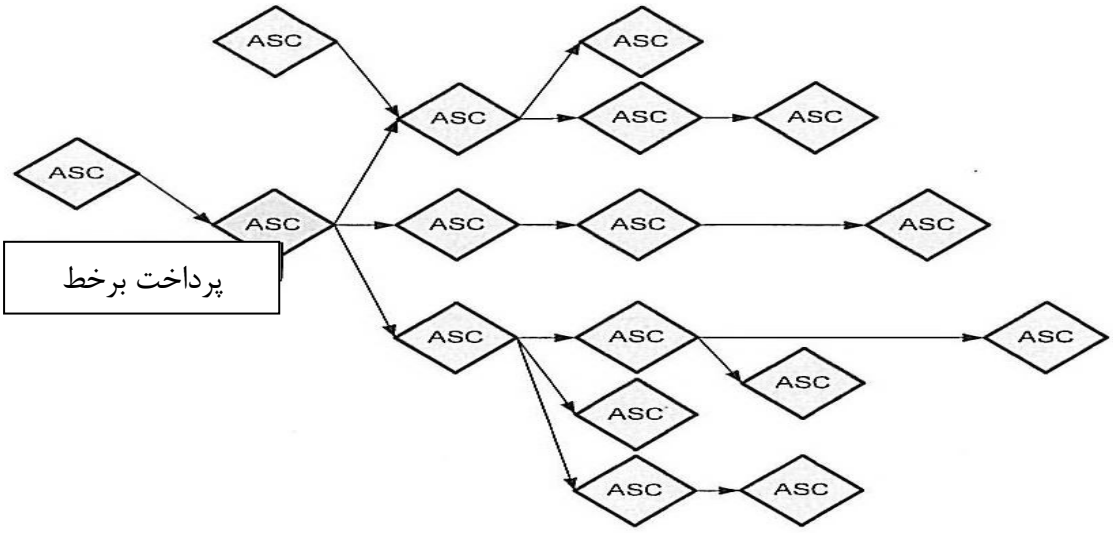
الف- تامین تنها اطلاعات مرتبط با کنشگرهای مختلف از طریق پنهان کردن پیچیدگی‌های غیرضروری

ب- تسهیل ارتباطات از طریق گروه‌بندی ASCهای مرتبط تحت یک عنوان و با استفاده از واژگان مناسب. برای مثال، استفاده از زبان سطح کسب‌وکار هنگام برقراری ارتباط با مدیران

پ- تسهیل توزیع ASCها از طریق گروه‌بندی آن‌ها در مجموعه‌های مرتبط

ت- تضمین این‌که تمام فعالیت‌های امنیتی در ASCهای متصل اجراشده و هیچ‌کدام کنار گذاشته نشده‌اند.

شکل۷ مثالی از این رابطه گراف را نشان می‌دهد که در آن مجموعه‌ای از ASCها تحت عنوان «پرداخت برخط» به هم متصل شده‌اند. در این مثال، تمام ASCهای مربوط به پرداخت اینترنتی می‌توانند به‌عنوان مجموعه‌ای واحد استفاده شوند و در صورت لزوم این پیچیدگی پنهان شود.



شکل ۷- گراف ASCها

ASC ساختار داده‌ای پیچیده‌ای است که جزئیات بیشتر آن در مستند ‹‹ قسمت ۵- پروتکل‌ها و ساختار داده ASC›› مطرح خواهد شد. مرور کلی مختصری در زیر آمده است.

یادآوری - هرچند استاندارد ISO/IEC 27034-5 ساختار ASC را رسمی خواهد کرد، اما ممکن است سازمان‌ها هنوز برای راهنمایی در مورد مشخص کردن اقلام 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 حاوی اطلاعاتی از قبیل موارد زیر است:

الف- اطلاعات ASC: نام، شناسه، مؤلف، تاریخ و توصیف ASC

ب- نشانگرهایی به ASCهای والد و ASCهای فرزند (یک ASC تواند به‌صورت ساختار گراف ارائه شود.)

پ- نشانگرهایی به زمینه‌های کسب‌وکار، مقرراتی و فناورانه مرتبط و همچنین مشخصاتی از برنامه کاربردی که نیازهای امنیتی این ASC را فراهم می‌کنند.

۸-۱-۲-۶-۵-۳ هدف ASC

هدف ASC، دلیل وجود ASC یعنی نیازهای امنیتی که این ASC برای آن‌ها طراحی‌شده است را مشخص می‌کند.

هدف ASC موارد زیر را مشخص می‌کند:

الف- کدام‌یک 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 نیازهای برنامه کاربردی که این ASC به آن‌ها مربوط می‌شود و می‌توانند به مقرراتی، 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 تعریف‌شده است. این ASC برای تمام پروژه‌هایی ضروری است که برنامه کاربردی درگیر در پرداخت اینترنتی را توسعه می‌دهند و سطح اعتماد هدف‌گذاری‌شده توسط مالک برنامه کاربردی از ۱ تا ۲ مقررشده است. اگر مالک برنامه خواهان مقرر کردن سطح اعتماد هدف‌گذاری‌شده ۳ برای برنامه کاربردی باشد، یک ASC با فعالیت امنیتی قوی‌تر و/یا سنجش امنیت قوی‌تر موردنیاز است.

۸-۱-۲-۶-۵-۴ فعالیت امنیتی ASC

این عنصر گام‌ها یا روش‌های اجرایی لازم برای پیاده‌سازی فعالیت را توصیف می‌کند و توصیه می‌شود کمینه موارد زیر را تعریف کند:

الف- چه چیزی:

۱- توصیف کامل فعالیت امنیتی

۲- پیچیدگی فعالیت

۳- محصولات مصنوعی تولیدشده توسط فعالیت. این فراورده شواهد اثباتی لازم برای نشان دادن حضور برنامه کاربردی معرفی‌شده، فرایندها یا روش‌های اجرایی واپایش امنیت (برای مثال فعالیت ASC) را بیان می‌کند.

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

ب- چگونه :

فنون اجرای این فعالیت و به دست آوردن فراورده، مانند شناسایی کد منبع استفاده‌شده برای پیاده‌سازی ارتباطات امن با یک خدمت LDAP، شناسایی کتابخانه مورداستفاده قرارگرفته برای رمزبندی یا سندی که برای انجام فعالیت، راهنمایی فراهم می‌کند.

ج- کجا:

هدف فعالیت امنیتی، مانند کد منبع، پارامترهای برنامه کاربردی، مؤلفه‌های زیرساختی، فرایند

د- چه کسی:
صلاحیت‌های موردنیاز برای کنشگرهایی که توصیه می‌شود این فعالیت را اجرا کنند. ASCها به کنشگرها محول می‌شوند، (احتمالاً در شکل انتساب‌های رسمی سازمانی) زیرا توصیه می‌شود سازمان اطمینان حاصل کند که صلاحیت‌های حرفه‌ای هر نقش اکتساب‌شده‌اند و اصل تفکیک وظایف مورد ملاحظه قرارگرفته است. توصیه می‌شود ASCها 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 (به بند ۸-۱-۲-۷ مراجعه شود) که توصیه می‌شود این فعالیت در آن اجرا شود.
و) چقدر:
هزینه تخمینی انجام این فعالیت ASC.

۸-۱-۲-۶-۵-۵ سنجش درستی ASC

این بخش واپایش درستی را ارائه می‌دهد که برای درستی‌سنجی موفقیت اجرای فعالیت ASC مرتبط اجرا می‌شود. توصیه می‌شود سنجش درستی کمینه موارد زیر را تعریف کند:
الف- چه چیزی:
۱- توصیف کامل سنجش امنیت. این توصیف چگونگی درستی‌سنجی وجود و صحت فراورده تولیدشده توسط فعالیت ASC را نشان می‌دهد.
۲- پیچیدگی سنجش
۳- فراورده تولیدشده توسط این سنجش. این فراورده شواهد اثباتی لازم را بیان می‌کند تا نشان دهد ASC درستی‌سنجی‌شده است.
۴- نتایج مورد انتظار (موقعیت، وضعیت یا توصیف دقیق ارزش فراورده)
ب- چگونه:
فنون اجرای این سنجش و به دست آوردن فراورده مانند ابزارها و زمینه بازبینی کد یا سندی که راهنمایی اجرای سنجش را فراهم کند.
پ- کجا:
هدف فعالیت درستی‌سنجی، یعنی خصوصیات دقیق فراورده تولیدشده توسط فعالیت ASC مرتبط که مورد درستی‌سنجی قرار می‌گیرد.
ت- چه کسی:
صلاحیت‌های حرفه‌ای موردنیاز کنشگرهای درگیر در واپایش تأیید. ASCها به کنشگرها محول می‌شوند، (احتمالاً در شکل انتساب‌های رسمی سازمانی) زیرا سازمان توصیه می‌شود اطمینان حاصل کند که صلاحیت‌های حرفه‌ای هر نقش اکتساب‌شده‌اند و اصل تفکیک وظایف مورد ملاحظه قرارگرفته است. توصیه می‌شود ASCها برای مقصود صریح درستی‌سنجی صلاحیت‌های حرفه‌ای نوشته شوند.
ث- چه وقت:

اشـاره به یک فعالیت خاص در مـرحله‌ای از مدل مرجع چـرخه حیات امنیت بـرنامه کاربـردی (بند ۸-۱-۲-۷ مراجعه شود.) که این سنجش در آن توصیه می‌شود انجام گیرد. در صورت نیاز، این سنجش می‌تواند به‌صورت دوره‌ای برگزار شود.

ج- چقدر:

هزینه تخمینی یک‌بار رخداد این فعالیت سنجش درستی.

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

۸-۱-۲-۷-۱ کلیات

سازمانی که کسب‌وکار آن درگیر با تولید، برون‌سپاری یا اکتساب برنامه کاربردی است معمولاً چارچوبی از فرایندهای تعریف‌شده و فعالیت‌های طبقه‌بندی‌شده را به‌صورت مرحله‌ای استفاده می‌کند. این چارچوب «مدل چرخه حیات» نامیده می‌شود. با توجه به زمینه مورداستفاده، 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 ارائه‌شده باشد، بلکه تعریف آن را می‌توان در استانداردهای ISO/IEC 12207 و ISO/IEC5288 مشاهده نمود.

این‌گونه چارچوب برای هر سازمان منحصربه‌فرد و بومی‌سازی شده است و در طی سال‌ها استفاده و پالایش‌شده 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 ایجادشده‌اند. 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 انجام‌شده در طی مراحل چرخه حیات برنامه کاربردی یک نرم‌افزار یا یک سامانه، قسمتی از فرایند-های سطح سازمانی هستند که توصیه می‌شود با نیازهای الزامی ارائه‌شده 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 فرایندهای 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 واپایش امنیت برنامه کاربردی (ASC) به فعالیت‌های معمول در مراحل تعریف‌شده در مدل چرخه حیات برنامه کاربردی سازمان اضافه می‌کند.

همان‌گونه که قبلاً در بند 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 درستی توصیه می‌شود 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 غیرممکن است که یک ASC در استاندارد موجود باشد که مستقیماً به یک مرحله فرایند 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. راه‌حل این مشکل، ارائه یک مدل مرجع چرخه حیات امنیت برنامه کاربردی به‌عنوان یک مرجع استاندارد جهت اضافه کردنASCها به فعالیت‌های اجراشده درباره مدیریت برنامه کاربردی، تامین و عملیات 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 راهبری، نگهداری نرم‌افزار و زیرساخت، مدیریت پروژه، ممیزی و واپایش

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 فرایندها و کنشگرهای بالقوه مرتبط با امنیت برنامه کاربردی اعتبار بخشد.

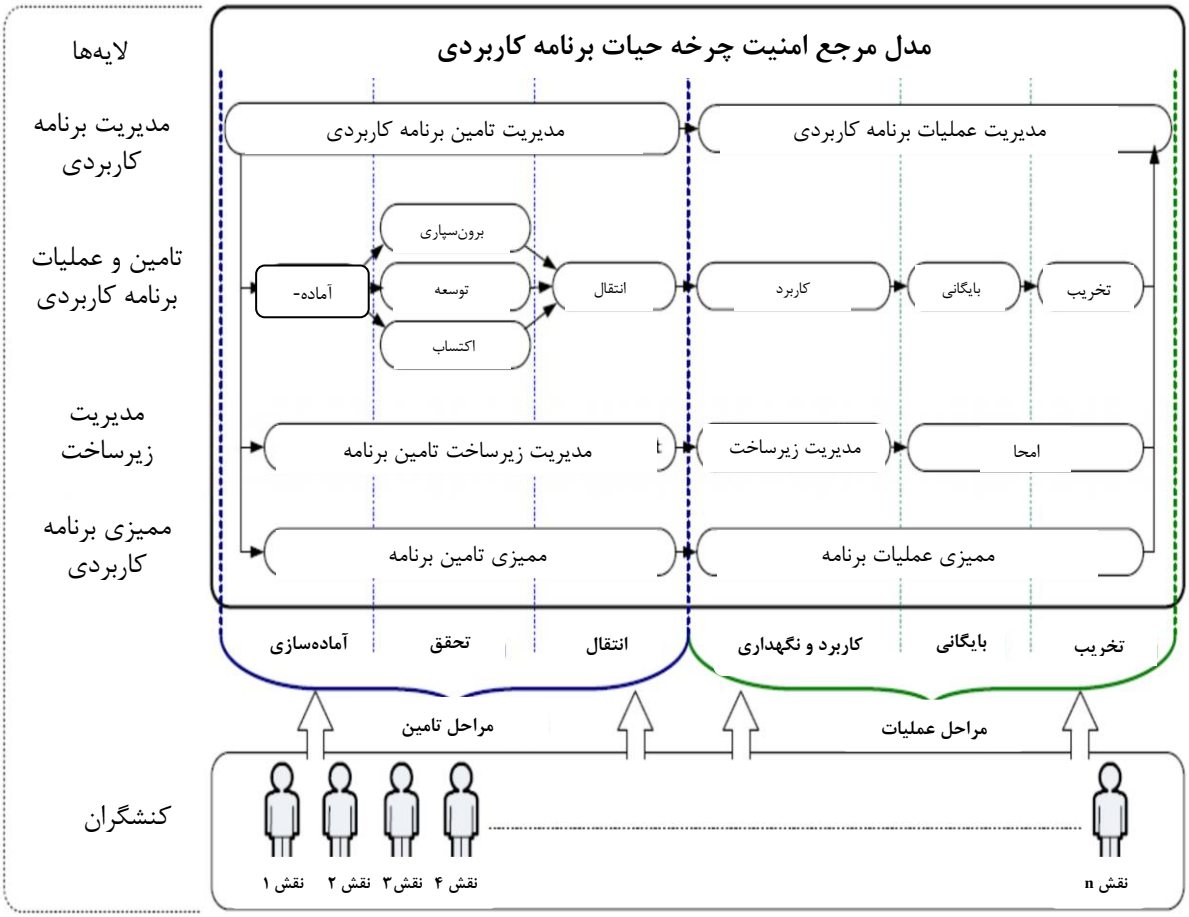
ب- به سازمان کمک کنند که توجه صحیح به تمام نگرانی‌های امنیتی در تمامی مراحل چرخه‌های حیاتی برنامه را تضمین کند.

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 کمینه برسانند.

ت- باوجود چرخه‌های حیات متفاوت برنامه کاربردی برای سازمان، مدلی استاندارد برای جهت به اشتراک‌گذاری ASCها بین گروه‌های پروژه فراهم می‌کند.

ث- باوجود چرخه‌های حیات متفاوت برنامه کاربردی، برای سازمان مدلی استاندارد برای جهت به اشتراک‌گذاری ASCها با سازمان‌های دیگر فراهم می‌کند.

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



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

توصیه می‌شود سازمان ارتباطی پایدار بین مراحل و فعالیت‌های تعریف‌شده در این مدل مرجع و مراحل و فعالیت‌های مورداستفاده 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 کمینه قابل‌قبول جهت سطح اعتماد هدف‌گذاری‌شده را در طول راه‌اندازی برنامه‌ریزی تمام پروژه‌های برنامه کاربردی سازمان تضمین می‌کند.

مدل مرجع به‌طور افقی به دو قسمت تقسیم‌شده است: تامین، که در آن فعالیت‌ها جهت به دست آوردن و اجرای برنامه انجام می‌شوند و عملیات که فعالیت‌های پس از توزیع آن انجام می‌شوند.

مراحل تامین و عملیات می‌توانند به مراحل بیشتر که در زیر آمده است تقسیم شوند:

الف- مراحل تامین شامل سه مرحله: آماده‌سازی، تحقق و انتقال،

ب- مراحل عملیات شامل سه مرحله: کاربرد و نگهداری، بایگانی و امحا[1] .
مدل مرجع به‌صورت عمودی به چهار لایه اصلی تقسیم می‌شود:
الف- مدیریت برنامه: این لایه از فعالیت‌های در زمینه راهبری، مانند مدیریت پروژه و مدیریت عملیات برنامه تشکیل‌شده است. این فعالیت‌ها در حیطه فرایندهای تعریف‌شده در ISMS سازمان انجام می‌پذیرند.
ب- تامین و عملیات برنامه کاربردی: این لایه از فعالیت‌های مربوط به تهیه و استفاده از خود برنامه کاربردی تشکیل‌شده است. این فعالیت‌ها معمولاً در حیطه فرایندهای پیشنهادی استانداردهایی مانند سری استاندارد ISO/IEC 15026، استاندارد ISO/IEC 5288، استاندارد ISO/IEC 12207 و استانداردISO/IEC 21827 انجام می‌پذیرند.
ج- مدیریت زیرساخت: این لایه از فعالیت‌های مربوط به مدیریت خدمات IT در سازمان تشکیل‌شده است که از برنامه پشتیبانی می‌کنند. این فعالیت‌ها معمولاً در حیطه فرایندهای پیشنهادی استانداردهایی مانند استاندارد TR 20000-4 و محصولات راهنما مانند ITIL انجام می‌پذیرند.
د- بازبینی برنامه: این لایه متشکل از فعالیت‌های مربوط به واپایش 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 داده‌شده به‌طور زیر توصیف می‌شوند.

۸-۱-۲-۷-۲ مدیریت تامین برنامه کاربردی

فعالیت‌های مربوط به مدیریت تامین برنامه کاربردی توسط مدیران پروژه و مدیران اداری در طی مراحل تامین از چرخه حیاتی برنامه اجرا می‌شوند.
این‌گونه فعالیت‌ها به‌عنوان قسمتی از فرایندها در سطح سازمان اجرا می‌شوند و شامل فرایندهای مهندسی نرم-افزار از گروه فرایندهای پروژه تعریف‌شده در استاندارد ISO/IEC 12207 از قبیل فرایند مدیریت منابع انسانی، فرایند برنامه‌ریزی پروژه ، فرایند ارزیابی و واپایش پروژه و فرایند مدیریت تصمیم‌گیری است.

۸-۱-۲-۷-۳ مدیریت عملیات برنامه کاربردی

فعالیت‌های مدیریت عملیات 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.

1- Destruction

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، توصیه می‌شود 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 کاربردی، ISMS سازمان را به همراه شواهد و تضمین مورد نیاز حاکمیت پروژه، فراهم می‌شود.

۸-۱-۲-۷-۴ آماده‌سازی

گروه تامین، در طی مرحله آماده‌سازی، فعالیت‌های اولیه یا آماده‌سازی را انجام می‌دهد. این فعالیت‌ها معمولاً قسمتی از فرایند در سطح سازمانی هستند. ازجمله فرایندهای مهندسی نرم‌افزار استاندارد ISO/IEC 12207 مانند بند ۶-۳-۳، فرایند مدیریت تصمیم‌گیری و بند ۶-۳-۶، فرایند مدیریت اطلاعات.

۸-۱-۲-۷-۵ فرایندهای آماده‌سازی

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

یادآوری- این فرایند شامل فرایندهای مهندسی نرم‌افزار بخش ۶-۴-۱ استاندارد ISO/IEC 12207 فرایند تامین 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 گروه تامین به اجرا درمی‌آیند. 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 برون‌سپاری 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 گروه تامین در طی مرحله تحقق انجام می‌گیرد. چنانچه سازمان در حال اجرای برخی فعالیت‌های پیاده‌سازی به‌صورت داخلی باشد، ممکن است ASCهای اضافه‌شده به این فعالیت‌های پیاده‌سازی با ASCهای اضافه‌شده هنگام خرید یا برون‌سپاری پیاده‌سازی یا مؤلفه‌های 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 دربرگیرنده فرایندهای مهندسی نرم‌افزار در استاندارد ISO/IEC 12207 ازجمله فرایند مدیریت مخاطره، طراحی معماری سامانه، فرایند طراحی معماری سامانه، جزئیات فرایند طراحی نرم‌افزار، فرایند ساخت نرم‌افزار، فرایند مدیریت اسناد نرم‌افزاری، 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 گروه تامین و به‌منظور به دست آوردن یا خرید محصول یا خدمات موردنیاز 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 به‌دست‌آمده می‌شوند، ارائه می‌کنند.

این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندهای در سطح سازمان هستند و دربرگیرنده فرایندهای مهندسی نرم‌افزار از استاندارد ISO/IEC 12207 ازجمله 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 گروه تامین 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 ازجمله 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، ازجمله 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 گروه عملیات در هنگامی‌که برنامه دیگر در حالت عملیاتی موردنیاز نیست، انجام می‌شوند. این فعالیت‌ها شامل بایگانی تمام اطلاعات نرم‌افزار ازجمله بایگانی تمام ابزارها و فرایندها به‌منظور حفاظت و دسترسی امن به اطلاعات هستند، حتی درزمانی 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 ازجمله فرایند امحای نرم‌افزار هستند.

۸-۱-۲-۷-۱۲ تخریب

فعالیت‌های تخریب در تخریب امن تمام اطلاعات برنامه کاربردی ازجمله 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 ازجمله فرایند امحای نرم‌افزار هستند.

۸-۱-۲-۷-۱۳ مدیریت زیرساخت تامین برنامه کاربردی

این قسمت از فعالیت‌ها در مرحله تامین شامل فعالیت‌های مرتبط با تهیه و نگهداری یک زیرساخت فناوری امن در پشتیبانی از فعالیت‌های گروه تامین 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 اجراشده و دربرگیرنده فرایندهای مهندس نرم‌افزار از استاندارد ISO/IEC 12207 ازجمله فرایند مدیریت زیرساخت و فرایند مدیریت پیکربندی است.

۸-۱-۲-۷-۱۴ مدیریت زیرساخت عملیات برنامه کاربردی

این قسمت از فعالیت‌ها در مرحله تامین 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.

توصیه می‌شود فعالیت‌های دیگر در طی مراحل عملیات جهت نگهداری امن زیرساخت پشتیبان برنامه انجام شوند. نگهداری زیرساخت 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 اجراشده و دربرگیرنده فرایندهای مهندسی سامانه استاندارد ISO/IEC 5288 ازجمله فرایند عملیات و فرایند نگهداری هستند.

۸-۱-۲-۷-۱۵ امحا

فعالیت‌های امحای برنامه کاربردی جهت ارائه تضمین این‌که اطلاعات ذخیره‌شده بر روی کارسازها، سامانه‌ها و سایر مؤلفه‌های فنی مورداستفاده یک برنامه کاربردی به شکل امن پاک‌شده‌اند، اجرا می‌شوند. این امر اجازه می‌دهد سازمان بدون مخاطرات امنیتی این مؤلفه‌ها 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 ممیزیِ تامین برنامه کاربردی

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

این فعالیت‌ها بر اساس سطح اعتماد هدف‌گذاری‌شده پروژه برنامه کاربردی ممکن است یک‌بار یا به‌صورت دوره-ای توسط گروه‌های 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 اجراشده در مرحله تامین 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 تامین ارائه می‌کند.

این فعالیت‌ها معمولاً به‌عنوان قسمتی از فرایندها در سطح سازمان اجراشده و دربرگیرنده فرایندهای مهندسی نرم‌افزار از استاندارد ISO/IEC 12207، ازجمله فرایند ممیزی نرم‌افزار هستند.

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

فعالیت‌های ممیزی در طی مراحل عملیات برنامه کاربردی معمولاً مراحل تامین تفاوت دارند. سازمان‌هایی که با برنامه‌های اکتساب‌شده کار می‌کنند، ممکن است نیاز به ممیزی برنامه کاربردی در مراحل تامین 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 به‌عنوان قسمتی از فرایندها در سطح سازمان اجراشده و دربرگیرنده فرایندهای مهندسی نرم‌افزار استاندارد ISO/IEC 12207 ازجمله فرایند ممیزی برنامه کاربردی هستند.

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

ONF انباره کلیه فرایندهای مورداستفاده سازمان است. بنابراین توصیه می‌شود کلیه فرایندهای مربوط به تعریف مدیریت و تأیید صلاحیت امنیت برنامه کاربردی به‌طور رسمی در ONF توصیف شوند.

ازجمله:

الف- تمام فرایندهای توصیف‌شده دربند ۸ این استاندارد ملی

ب- تمام فرایندهای تعریف‌شده در قسمت‌های بعدی استاندارد ISO/IEC 27034

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

۸-۱-۳ فرایندهای مربوط به چارچوب الزامی سازمان

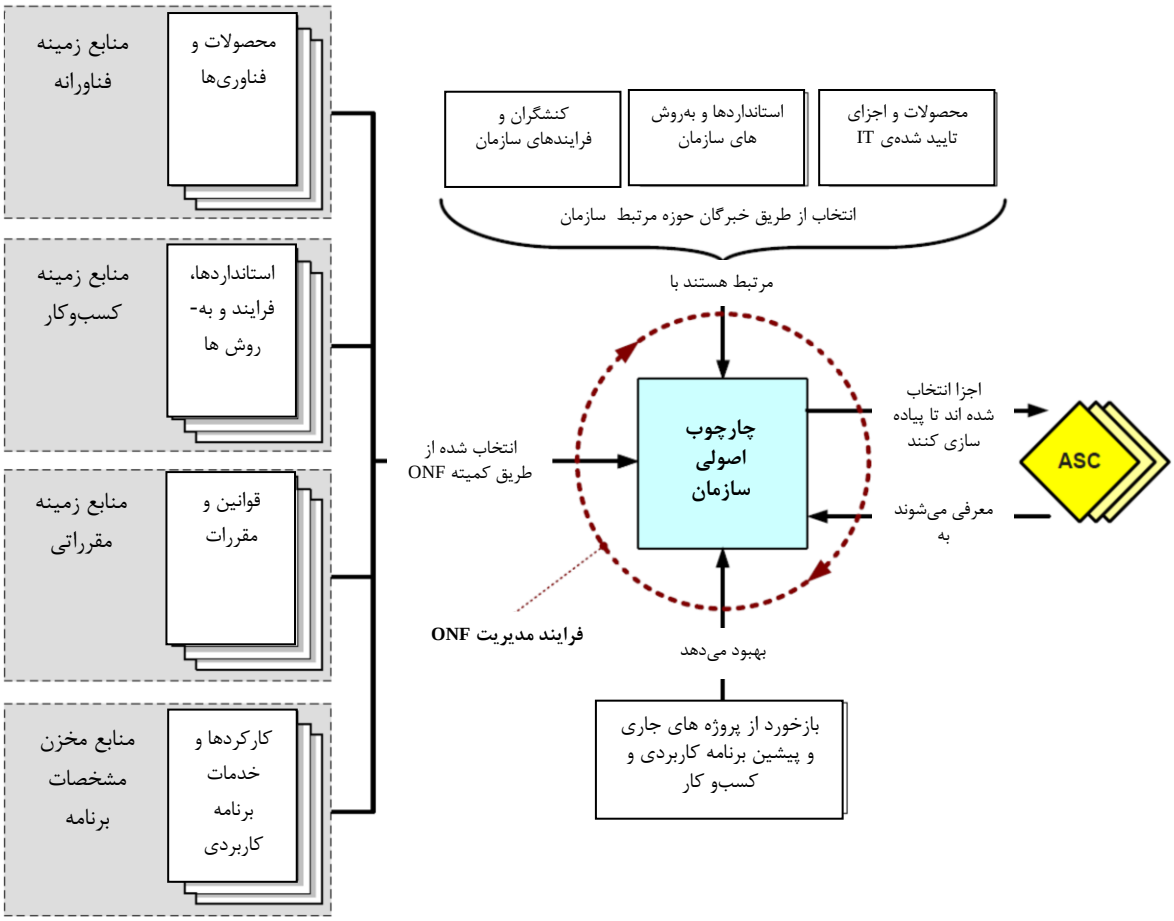
۸-۱-۳-۱ کلیات

زمینه‌سازمانی در طول زمان تکامل می‌یابند، به همین دلیل توصیه می‌شود مؤلفه‌های ONF معرف این زمینه‌ها مانند زمینه فنی، کسب‌وکار و مقرراتی و خصوصیات برنامه کاربردی به‌روز باشند.

توصیه می‌شود کمیته ONF فرایندهای ایجاد، تأیید و نگهداری ONF و تمام مؤلفه‌های آن را تعریف، ثبت و تصویب کند. توصیه می‌شود نقش‌ها مسئولیت‌ها و صلاحیت‌های حرفه‌ای کنشگرهای درگیر در جریان فرایندها نیز مشخص شود. به‌عنوان‌مثال شکل ۹ نمای کلی از فرایند نگهداری ONF را نشان می‌دهد.

این فرایندها در شمای کلی حاضر ارائه‌شده و به‌تفصیل در استاندارد ISO/IEC 27034-2 موردبحث 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 داده‌شده، به‌طور موازی با آن‌ها اجرا می‌شوند.

اهداف فرایند مدیریت ONF عبارت‌اند از :

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

ب- تضمین این‌که مؤلفه‌های ONF جهت بازتاب تغییرات واقع‌شده در خارج از سازمان به‌روز هستند. به‌عنوان‌مثال تغییر در قوانین می‌تواند باعث تغییر زمینه مقرراتی در ONF شود.

پ- اکتساب تأییدیه از مدیران عالی در مورد خط‌مشی‌های امنیتی در سطح سازمان و مدیران ارشد در مورد اهمیت تمامی مؤلفه‌های ONF

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

ث- ارسال مؤلفه‌های ONF به تمام گروه‌ها در سازمان

ج- ارائه بازخورد به ONF جهت پوشش دانش جدید پیشنهادها، در مورد پیشرفت ASC روش‌های جدید به‌دست‌آمده در طول یک پروژه برنامه کاربردی

۸-۱-۳-۳ فرایندهای فرعی مدیریت ONF

توصیه می‌شود تمامی فرایندهای مرتبط به امنیت برنامه‌های کاربردی 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 هم‌جهت می‌شوند.

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

فرایند ISMS	فرایند فرعی مدیریت ONF
طراحی	طراحی ONF
انجام	پیاده‌سازی ONF
بررسی	نظارت و بازبینی ONF
اجرا	بهبود مستمر ONF

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

الف – طراحی ONF :

۱- مشخص کردن و ثبت تمامی زمینه‌های ممکن (کسب‌وکار، مقرراتی و فنی) که برنامه کاربردی در آن‌ها مورداستفاده 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 بر اساس استاندارد ملی ۲۷۰۰۵

۴- تحلیل به‌روش‌ها و استانداردها مانند استاندارد ISO/IEC 12207 ، استاندارد ISO/IEC 5288 ، استاندارد ISO/IEC 15026 و تعریف ASCها بر اساس 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 بند ۸-۱-۲-۶-۵ مطرح‌شده تعیین کنند.

مثال ۱- یک ASC موردنیاز جهت اعمال امنیت برنامه کاربردی که باید توسط برنامه‌ریزی ارشد و باکفایت در یک‌زبان برنامه‌نویسی ویژه ایجاد یا به‌روزرسانی شود.

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

ب- اعتبارسنجی و یکپارچه‌سازی ASC

توصیه می‌شود گروه 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 قابل‌فهم خواهد بود و نیز تأیید کنند که این ASC درواقع مخاطره تعریف‌شده را کاهش می‌دهد. همچنین توصیه می‌شود گروه مذکور مشخص کنند این ASC برای کدام سطح اعتماد لازم است.

تأیید نهایی ASCCها 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 موردنیاز 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 مورداستفاده سازمان است.

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

ت- بهبود مستمر ONF: نگهداری و بهبود مؤلفه‌های 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 فرایند مدیریت مخاطره است که در استاندارد ملی ۲۷۰۰۵ توضیح داده شد. به‌این‌ترتیب، ارزیابی مخاطره امنیت برنامه کاربردی، مرحله دوم فرایند مدیریت امنیت برنامه کاربردی است و فرایند ارزیابی مخاطره را در سطح برنامه کاربردی اجرا می‌کند. دیگر مراحل مدیریت مخاطره توسط دیگر مراحل فرایند مدیریت امنیت برنامه کاربردی به اجرا درمی‌آیند.

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 درنهایت مخاطره‌های مشتق شده را اولویت‌بندی می‌کند و آن‌ها را بر اساس 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 سطح بالای مخاطره 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، مقرراتی و کسب‌وکار سطح هدف‌گذاری‌شده را تعریف می‌کند.

توصیه می‌شود مالک پروژه برنامه کاربردی خاص نقش مشخصی برای مسئولیت اجرای این تحلیل و با استفاده از روشگان مناسب برای تحلیل سطحی برنامه کاربردی مشخص کند. ممکن است روشگان تحلیل مخاطره سطح سازمانی برای این وظیفه کافی نباشد.

۸-۲-۲-۲ تحلیل تفصیلی مخاطره 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 مقرراتی برای برنامه کاربردی در سازمان موردنظر تأیید می‌کند.

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

توصیه می‌شود مالک پروژه برنامه کاربردی خاص ، نقش صریح با مسئولیت اجرای این تحلیل با استفاده از روشگان مناسب برای تحلیل در سطح برنامه در نظر گیرد. ممکن است روشگان تحلیل مخاطره سطح سازمانی برای این وظیفه کافی نباشد.

۸-۲-۳ ارزیابی مخاطره

طبق استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲، « ارزیابی مخاطره، با استفاده از درکی که تحلیل مخاطره از مخاطرات فراهم آورده است، نسبت به اقدامات آینده تصمیم می‌گیرد. توصیه می‌شود این تصمیمات 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 هدف‌گذاری‌شده را می‌گیرد که خود تعیین می‌کند کدام‌یک از واپایش‌های امنیت برنامه کاربردی توصیه می‌شود برای حل مخاطره به کار گرفته شوند.

۸-۲-۴ سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی

سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی می‌تواند در دست‌یابی به سطح اعتماد موردنظر سازمان کمک کند تا برنامه پس از پذیرفته شدن مخاطرات مشخص‌شده در ارزیابی مخاطره به شیوه‌های امن مورداستفاده قرار گیرد.

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

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

توصیه می‌شود سطح اعتماد ایده آل برنامه یکی از سطوح اعتمادی باشد که در گنجینه سازمانی واپایش امنیت برنامه تعریف‌شده است.

کتابخانه واپایش امنیت برنامه (شکل ۵) را می‌توان به شکل جدولی نشان داد که در این صورت، سطح اعتماد ایده آل برنامه، ستونی از آن خواهد بود. به‌این‌ترتیب انتخاب یک سطح اعتماد، گزینش تمام واپایش 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 موردبررسی را دارد.

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

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

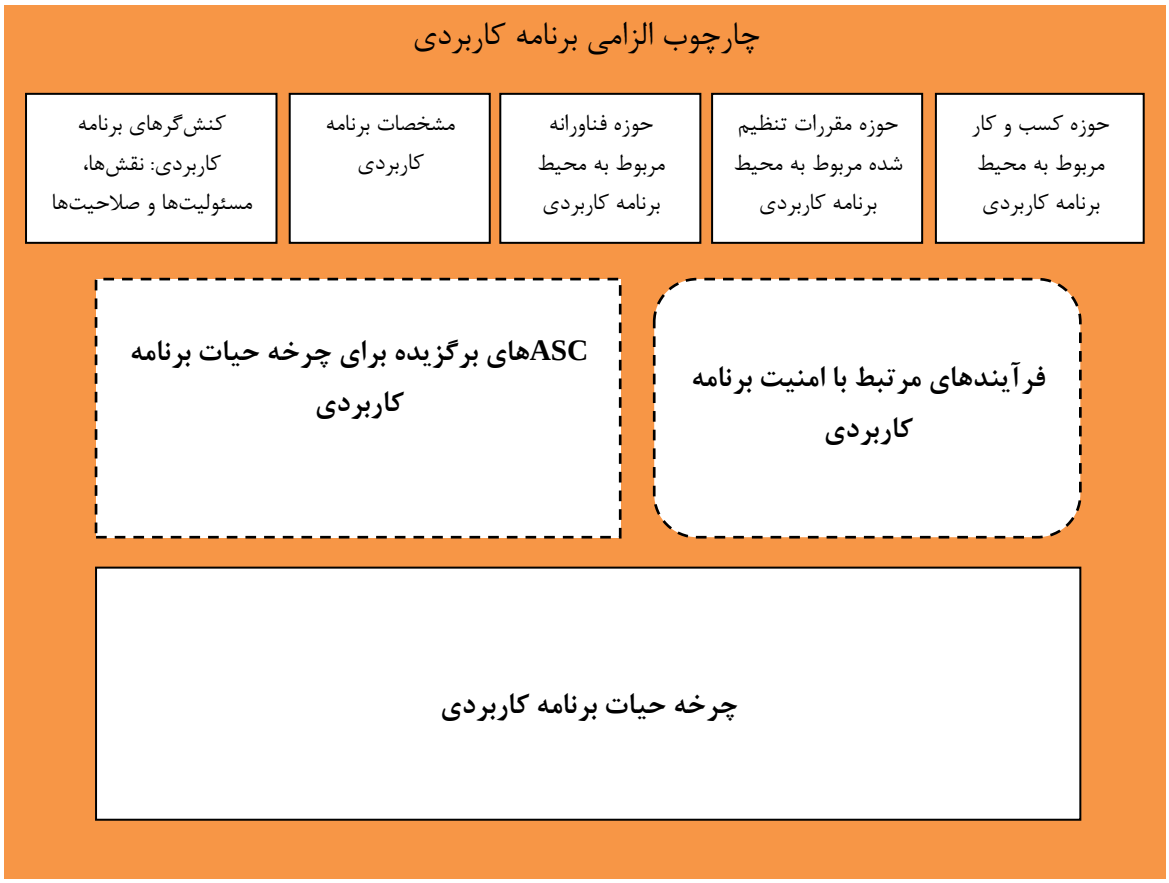
ب. تأیید نتایج ممیزی امنیت برنامه کاربردی در مرحله پنجم فرایند مدیریت امنیت برنامه کاربردی که طی آن سطح اعتماد واقعی برنامه سنجیده و با سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی مقایسه می‌شود. این

مرحله می‌تواند در هرزمانی 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 واپایش 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 موردنیاز برنامه کاربردی خاص را برای رسیدن به سطح اعتماد هدف‌گذاری‌شده توسط مالک برنامه کاربردی در جریان عنصر فرایند پذیرش گام دوم ASMP شامل می‌شود.
نیازهای امنیتی ANF از ارزیابی مخاطراتی مشتق می‌شوند که مربوط به استفاده سازمان از برنامه کاربردی اجرا-شده در گام دوم ASMP هستند.
برای هر پروژه برنامه کاربردی، ANF مرتبط با زمینه‌های فنی، مقرراتی و کسب‌وکار، 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 مقرراتی 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. توصیه می‌شود این تغییرات تأییدیه‌های مربوطه را از مالک برنامه کاربردی دریافت کنند.
ANF پروژه برنامه کاربردی خاص مؤلفه‌های تفصیلی زیر را شامل می‌شود. شکل ۱۰ نمایش نموداری ANF است.



شکل ۱۰- چارچوب الزامی برنامه کاربردی

۸-۳-۲ مؤلفه‌ها

۸-۳-۲-۱ زمینه کسب‌وکار مربوط به محیط برنامه کاربردی

تمام فرایندهای کسب‌وکار، روش‌ها، استانداردها و کنشگرهای درگیر در پروژه برنامه کاربردی، اعم از فرایندهای کسب‌وکار خارجی موردنیاز برای فراهم‌شده یکپارچگی کسب‌وکار مناسب در محیط اجرایی از زمینه کسب‌وکار ONF سازمان (به بند ۸-۱-۲-۱ مراجعه شود.) مشتق و بر اساس آن تصحیح می‌شوند.

۸-۳-۲-۲ زمینه مقرراتی مربوط به محیط برنامه کاربردی

تمام نیازهای قانونی و مقرراتی قابل کاربری درجایی که برنامه مورداستفاده مفید قرار می‌گیرد از زمینه مقرراتی ONF سازمان (به بند ۸-۱-۲-۲ رجوع کنید.) مشتق و بر اساس آن تصحیح می‌شوند.

۸-۳-۲-۳ زمینه فناورانه مربوط به محیط برنامه کاربردی

تمام مؤلفه‌های فنی برنامه کاربردی از قبیل معماری، زیرساخت، پروتکل‌ها و زبان‌ها از زمینه فنی ONF سازمان (به بند ۸-۱-۲-۴ مراجعه شود.) مشتق و بر اساس آن تصحیح می‌شوند.

۸-۳-۲-۴ مشخصات برنامه کاربردی

ویژگی‌های برنامه به سه شکل کارکردی، غیر کارکردی و نیازهای امنیتی درمی‌آیند.

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 استفاده‌شده توسط برنامه کاربردی را شامل می‌شود. این امر در مورد داده‌های خروجی برنامه نیز صدق می‌کند.

۸-۳-۲-۵ کنشگرهای برنامه کاربردی: نقش‌ها، مسئولیت‌ها و صلاحیت‌ها

توصیه می‌شود تمام عواملی که با برنامه کاربردی و در جریان چرخه حیات برنامه کاربردی با برنامه کاربردی در ارتباط هستند مشخص شوند. کنشگرها شامل: کارکنان امنیتی، مالکان برنامه کاربردی، مدیران پروژه، کارکنان ممیزی، معماران، آزمایندگان، توسعه‌دهندگان، کاربران نهایی، راهبران، راهبران دادگان و متخصصان فناوری می‌شوند.

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

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

الف- سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی

ب- نیازهای سازمان برای برنامه کاربردی

پ- زمینه و مشخصات خاص برنامه کاربردی

هر ASC همزمان فعالیتی 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 درمی‌آورند تا با بررسی شواهد اثباتی تأیید کنند فعالیت امنیتی مرتبط با موفقیت اجراشده است. همچنین توصیه می‌شود ASC نشانه‌هایی را برای مراحل خاصی از چرخه حیات برنامه کاربردی که فعالیت و سنجش موردنظر 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 آن ها را طراحی کنند. این رهیافت مداوم سازمان را در برخورد با نیازهای امنیتی برنامه کاربردی تأیید می‌کند.

توصیه می‌شود ASCهای برگزیده کمینه شامل تمام ASCهایی باشد که کمیته ONF برای سطح اعتماد صفر تصویب کرده است. توصیه نمی‌شود گروه پروژه در جریان پروژه برنامه کاربردی، ASCهای تصویب‌شده برای سطح اعتماد صفر را تغییر دهند.

۸-۳-۳ فرایندهای مرتبط با امنیت برنامه کاربردی

توصیه می‌شود مطابق این استاندارد ملی، ANF تمام فرایندهای مرتبط با تعریف، مدیریت و درستی‌سنجی امنیت برنامه کاربردی را شامل شود. این مسئله، همان‌گونه که در بند ۸-۱-۲-۸ توصیف‌شده، تصحیح جز «فرایندهای مربوط به امنیت برنامه کاربردی» ONF است.

۸-۳-۴ چرخه حیات برنامه کاربردی

چرخه حیات برنامه کاربردی مراحل و فعالیت‌های برگزیده از ONF را برای پروژه برنامه کاربردی خاصی به تصویر می‌کشد. به‌طور دقیق‌تر، چرخه حیات برنامه کاربردی زیرمجموعه‌ای از مدل مرجع چرخه حیات امنیت برنامه کاربردی است. (به بند ۸-۱-۲-۷ مراجعه شود.)

در مورد چرخه حیات برنامه کاربردی و همتای استاندارد آن، مدل مرجع چرخه حیات امنیت برنامه کاربردی، پیش‌تر در بند ۸-۱-۲-۷ صحبت شد.

سنجش‌ها و فعالیت‌های تعریف‌شده توسط ASC، از طریق فرایندهای متنوعی که در چرخه حیات برنامه کاربردی استفاده می‌شوند و گروه پروژه و درستی‌سنجی با آن‌ها آشنا هستند، اجرا می‌شوند.

به‌این‌ترتیب یکپارچگی تدریجی ASCها به‌عنوان فرایندهای یکپارچه استفاده‌شده در چرخه حیات برنامه کاربردی نسبت به فعالیت‌های امنیتی خارجی مجزا ارجحیت دارد.

۸-۳-۵ فرایندها

۸-۳-۵-۱ فرایندهای مرتبط با چارچوب الزامی برنامه کاربردی

توصیه می‌شود سازمان فرایندهای ایجاد، تأیید و نگهداری ANF را تعریف و ثبت کند. توصیه می‌شود نقش‌ها، مسئولیت‌ها و صلاحیت‌های حرفه‌ای موردنیاز عوامل درگیر در ANF برنامه کاربردی خاص مشخص شوند.

فرایند ایجاد ANF برنامه کاربردی خاص، فرایندی حیاتی است. این فرایند اطلاعات کلی موجود در ONF را به اطلاعات خاص موردنیاز ANF برنامه کاربردی خاص و نیازهای آن تبدیل می‌کند.

درحالی‌که ASCهای موجود در ONF به مراحل مدل مرجع چرخه حیات امنیت برنامه کاربردی متصل هستند، ASCهای ONF به مراحل چرخه حیات برنامه کاربردی خاص متصل هستند.

۸-۳-۵-۲ فرایند بازخورد

توصیه می‌شود سازمان فرایندی را برای بهبود دائم ONF از طریق بازخورد دانش جدید، پیشنهادهای بهبود واپایش امنیت برنامه کاربردی و روش‌های به‌دست‌آمده در زمان توسعه و استفاده مفید از برنامه کاربردی، تعریف کند.

این فرایند در شکل ۳ با عنوان‹‹ بازخورد فراهم‌شده›› نشان داده‌شده است.

توصیه می‌شود این فرایند با فرایند نگهداری ANF که در شکل ۹ با عنوان ‹‹بازخوردهای کسب‌وکار پیشین و جاری و پروژه‌های برنامه کاربردی›› نشان داده‌شده است، تلفیق شود.

۸-۴ تامین و عملیات برنامه کاربردی

۸-۴-۱ کلیات

مرحله چهارم ASMP شامل استفاده مفید و پیگیری در پروژه برنامه کاربردی ASCهای خاص می‌شود که توسط ANF فراهم‌شده است. گروه پروژه کاربری به‌طور خاص فعالیت‌های امنیتی خاص توصیف‌شده در قسمت ‹‹فعالیت امنیتی›› ASC را (همان‌گونه که در بند ۸-۱-۲-۶-۵-۴ توضیح داده‌شده است.) برای هر ASC موجود در AFN پیاده‌سازی می‌کند.

این مرحله برای گروه پروژه و گروه درستی‌سنجی، با فراهم آوردن ASCهای موردنیاز برای دست‌یابی به سطح اعتماد هدف‌گذاری‌شده آسان‌تر می‌شود. نیازی نیست که گروه‌ها از فرایندهایی که به ANFها منجر می‌شوند آگاه باشند.

ASC برای مدیران پروژه ابزار مفیدی خواهد بود. واپایش امنیت برنامه وظایف، منابع و صلاحیت‌های موردنیاز، هزینه هر وظیفه بر پایه روز- فرد و دقیقاً مرحله‌ای از چرخه حیات که توصیه می‌شود فعالیت در آن صورت بگیرد را به‌طور مفصل شرح می‌دهد.

ASC برای گروه درستی‌سنجی نیز ابزاری مفید خواهد بود زیرا اطلاعات دقیق مربوط به این‌که توصیه می‌شود چه نوع درستی‌سنجی اجرا شود تا ثابت کند فعالیت‌های امنیتی اجراشده و دست‌یابی به نتایج موردنظر مناسب است را فراهم می‌کند. این مسئله کمک می‌کند، گروه سنجش صحت از مطابقت برنامه کاربردی با نیازهای امنیتی اعتماد حاصل کنند.

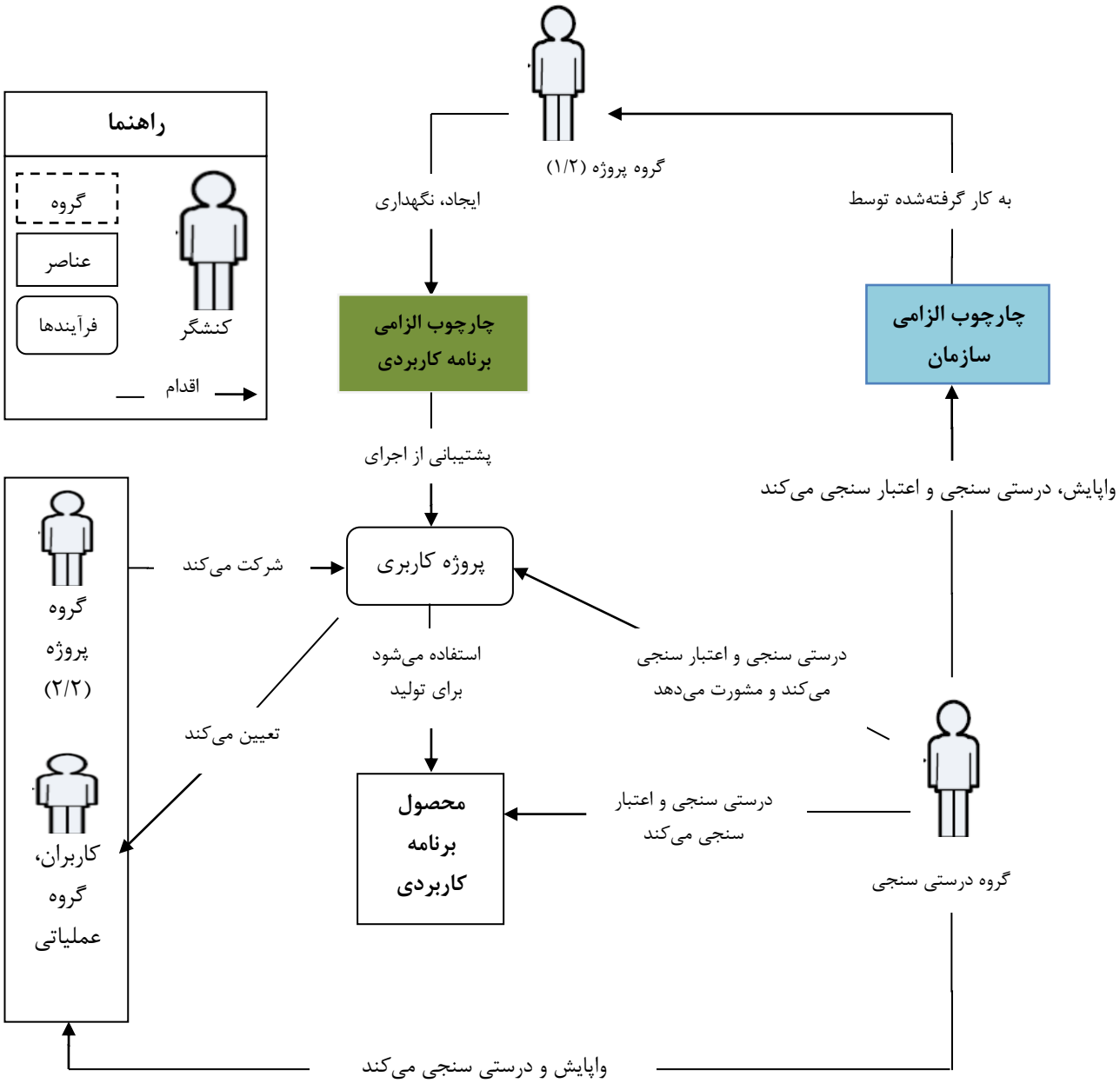
ASC برای گروه‌های امنیتی و فنی نیز مفید خواهد بود زیرا ASC موجود در ANF خاص فهرست مفصلی از نیازهای امنیتی را ارائه می‌دهد و به این شکل برنامه‌ریزی پیشرفته منابع موردنیاز را ممکن می‌سازد.

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

هر پروژه برنامه کاربردی معمول (پیش از پیاده‌سازی استاندارد ISO/IEC27034) توسط گروه پروژه، با پشتیبانی فرایندها و خودکار شدن توسط فناوری باهدف ایجاد یک برنامه هدایت می‌شود. اغلب، گروه تضمین کیفیت برنامه کاربردی، برنامه آزمایش را برای درستی‌سنجی کارکردهای برنامه کاربردی در مقابل نیازهای کارکردی موردپذیرش دنبال می‌کنند.

خود فناوری، روش‌های مورداستفاده گروه پروژه، تکمیل فرایند، کیفیت محصولات مصنوعی تولیدشده و کیفیت کنشگرهای درگیر در پروژه به‌ندرت درستی‌سنجی می‌شوند و چنانچه فرایند درستی‌سنجی اجرا شود به شکل رسمی تعریف نمی‌شوند.

شکل ۱۱ چگونگی تأثیر استاندارد ISO/IEC27037 در اضافه کردن نقش‌ها، مسئولیت‌ها، مؤلفه‌ها و فرایندها را در یک پروژه برنامه کاربردی نشان می‌دهد.



شکل ۱۱- تأثیر استاندارد ISO/IEC 27034 بر نقش‌ها و مسئولیت‌ها در یک پروژه برنامه کاربری

شکل ۱۱ چگونگی مشخص کردن رسمی نقش‌ها و مسئولیت‌ها 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 واپایش‌های 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 (بند ۸-۴-۴-۲ را ببینید.) بلکه در سطح سازمانی نیز به‌عنوان بخشی از فرایند ONF به اجرا درمی‌آید. (بند ۸-۱-۳-۳- ت را ببینید.)

۸-۴-۳ مؤلفه‌ها

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. ازجمله مهندسان معمار، تحلیل‌گران، برنامه‌نویسان و آزمایندگان.
این افراد مسئول گزینش عناصر ONF برای ایجاد یا نگهداری ANF پروژه برنامه کاربردی هستند.

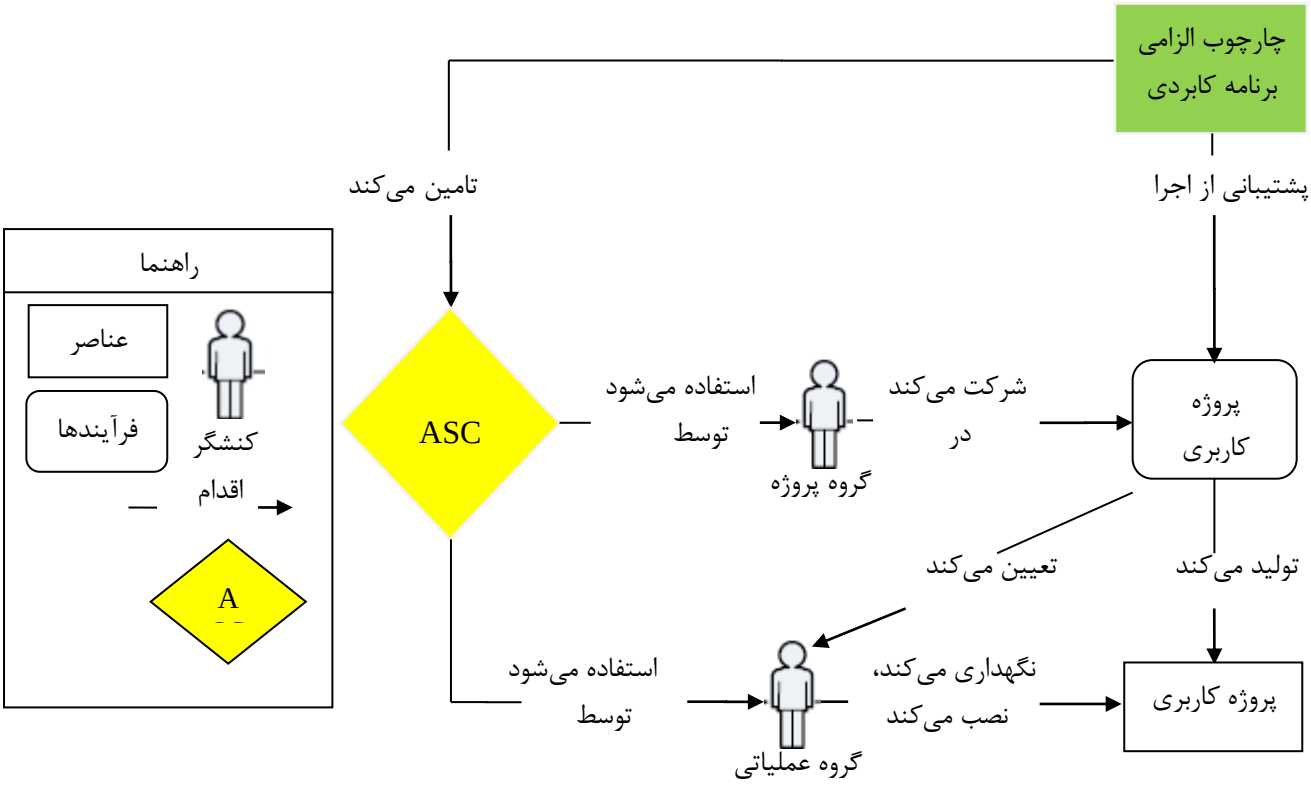
۸-۴-۳-۲ گروه عملیاتی

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

۸-۴-۴ فرایندها

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

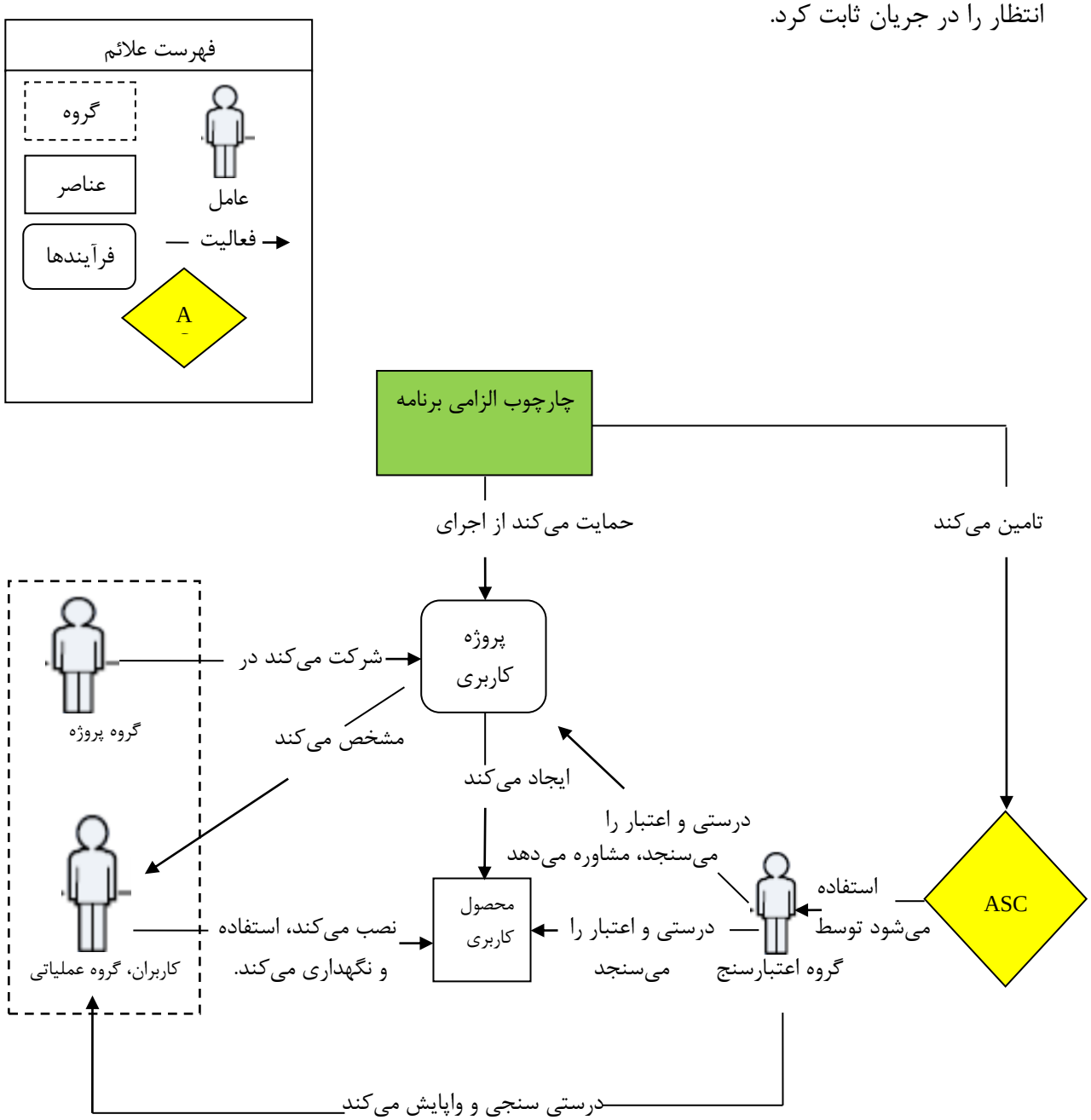
شکل ۱۲ نحوه استفاده گروه پروژه و گروه عملیاتی را از ASC به‌عنوان ابزاری برای اجرای فعالیت‌های امنیتی پروژه‌ای خاص نشان می‌دهد. فقط ASC موجود در ANF در این پروژه مورداستفاده قرار می‌گیرد.



شکل ۱۲- واپایش امنیت برنامه کاربردی به کار گرفته‌شده به‌عنوان فعالیت امنیتی

۸-۴-۴-۲ انجام سنجش‌های درستی سنجی در جریان یک پروژه برنامه کاربردی

قسمت درستی سنجی ASC، اصولی را پیاده‌سازی می‌کند که توصیه می‌شود بر اساس آن‌ها تمام فعالیت‌های امنیتی درستی‌سنجی شوند تا بتوان اجرای صحیح فعالیت توسط عامل متخصص و دست‌یابی به نتایج مورد انتظار را در جریان ثابت کرد.



شکل ۱۳- واپایش امنیت برنامه کاربردی به کار گرفته‌شده به‌عنوان معیار سنجش

شکل ۱۳ نشان می‌دهد که قسمت درستی‌سنجی واپایش امنیت برنامه کاربردی به‌عنوان قسمت واپایشی در چرخه حیات برنامه کاربردی به کار گرفته می‌شود تا گروه درستی‌سنجی، 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 خوشه‌بندی کارساز را برای در دسترس بودن برنامه کاربردی لازم بداند. قسمت درستی‌سنجی ASC پیاده‌سازی صحیح این خدمت را واپایش کرده و می‌سنجد.

شکل ۱۳ همچنین نشان می‌دهد که درستی‌سنجی واپایش امنیت برنامه کاربردی می‌تواند برای تأیید صلاحیت-های عوامل اجرایی فعالیت‌های چرخه حیات برنامه کاربردی مورداستفاده قرار گیرد. برای مثال، واپایش امنیت برنامه کاربردی ممکن است پیاده‌سازی یکی از مؤلفه‌های حیاتی برنامه کاربردی را توسعه داده و لازم بداند. سنجش صحت واپایش امنیت برنامه کاربردی، صلاحیت‌های توسعه گری را می‌سنجد تا این جزء را پیاده‌سازی کند.

۸-۵ ممیزی امنیتی برنامه کاربردی

۸-۵-۱ کلیات

هدف پنجمین فرایند مدیریت امنیت برنامه کاربردی، سنجش درستی و ثبت رسمی این است که آیا برنامه کاربردی خاص به سطح اعتماد هدف‌گذاری‌شده دست‌یافته و آن را نگهداری می‌کند.

این مرحله از فرایند مدیریت امنیت برنامه کاربردی می‌تواند در هرزمانی در چرخه حیات برنامه کاربردی اجرا شود. بسته به سطح اعتماد هدف‌گذاری شده برنامه کاربردی این مرحله می‌تواند موردی، دوره‌ای یا موقعیتی باشد.

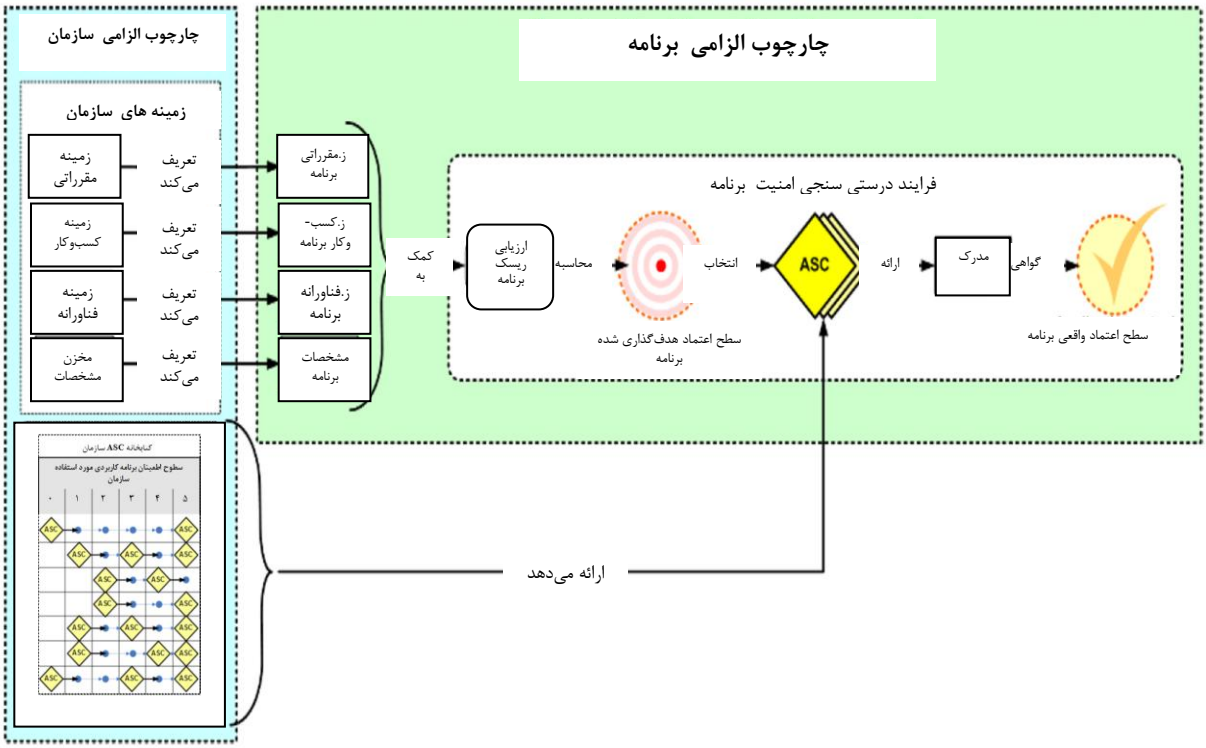
مثال ۱: سازمان می‌تواند این مرحله را به شکل دوره‌ای برای نظارت بر وضعیت پیاده‌سازی شده امنیت در مرحله تحقق برنامه کاربردی اجرا کند.

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 خط‌مشی‌های سازمانی موجود در ONF) اجرای تمام درستی‌سنجی‌های تعیین‌شده توسط واپایش امنیت برنامه را در چارچوب الزامی برنامه کاربردی و نتایج به‌دست‌آمده بررسی می‌کند. هدف این مرحله نمایش سطح اعتماد هدف‌گذاری‌شده برنامه کاربردی در مقطع زمانی خاص است. سازمان، زمانی می‌تواند برنامه کاربردی را امن معرفی کند که سطح اعتماد واقعی آن با سطح اعتماد هدف‌گذاری‌شده برابر شود.

این مرحله برابر با مرحله «پذیرش مخاطره» موجود در فرایند مدیریت مخاطره ذکرشده در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲است.



شکل ۱۴- مرورکلی فرایند درستی سنجی امنیت برنامه کاربردی

۸-۵-۲ مؤلفه‌ها

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

سطح اعتماد واقعی برنامه کاربردی بالاترین سطح اعتماد مشخص‌شده توسط گروه درستی‌سنجی بر اساس سنجش درستی‌سنجی تمام واپایش‌های امنیت‌های برنامه کاربردی است.

هر یک از واپایش‌های امنیت برنامه کاربردی موجود در چارچوب الزامی، شامل عملکرد درستی‌سنجی مفصلی است که باید توسط گروه درستی‌سنجی اجرا شود و مرحله موردنظر در چرخه حیات برنامه کاربردی را برای اجرای این سنجش مشخص می‌کند.

سطح اعتماد واقعی برنامه کاربردی با سنجش واپایش امنیت برنامه کاربردی به دست می‌آید که واپایش امنیت برنامه کاربردی نیز باید به‌نوبه خود در مقطع خاصی از چرخه حیات برنامه کاربردی کامل شود. چنانچه واپایش امنیت برنامه کاربردی در درستی‌سنجی 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 موردنظر را برای تمامی واپایش امنیت برنامه کاربردی مورد انتظار تأیید کنند.

بعدازاین تأیید، برنامه کاربردی، توسط سازمان امن در نظر گرفته‌شده‌اند 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 نیازهای 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 مؤلفه‌ها و فرایندهای این استاندارد ملی نگاشت پیدا می‌کند. این مطالعه موردی فرض می‌کند که تمام فعالیت‌ها و نتایج عملکرد باید مطابق با این استاندارد ملی باشد، مگر در مواردی که به‌طور خاص اشاره شد.

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، کسب‌وکار و مقرراتی 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 واپایش‌های 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 واپایش در این بخش طبق این استاندارد ملی در شکل زیر برای هر قسمت اشاره‌شده است. سپس هر یک از آن‌ها با یک مثال از کاربرد آن دنبال می‌شود. درجاهایی که ممکن است، ارجاع به منابع عمومی اطلاعات ارائه‌شده است. پیونده وب‌ها برای توصیف ویژه فرایندها، ابزارها و اطلاعات جانبی دیگر می‌تواند به‌وسیله این استاندارد ارائه شود.

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

درحالی‌که شرح 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 ISO تأیید نمی‌شود.

الف-۲ چرخه توسعه امنیت

چرخه توسعه امنیت، یک نرم‌افزار تضمین رویه امنیتی است. به‌عنوان یک ابتکار و یک خط‌مشی اجباری از سال ۲۰۰۴، چرخه توسعه امنیت نقشی حیاتی در تعبیه امنیت و حریم خصوصی در نرم‌افزار و شرکت‌های پذیرفته‌شده 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 حذف‌شده‌اند.

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

پاسخگویی	انتشار	درستی سنجی	پیاده‌سازی	طراحی	نیازها	آموزش
- اجرای پاسخگویی	- واکنش به طرح - بررسی نهایی میزان امنیت - بایگانی	- آزمون پویایی - درستی سنجی مدل و خطرات بررسی سطحی	- تعیین ابزارها - جلوگیری از انجام موارد ممنوعه - تحلیل ایستا	- خطر تحلیل سطحی - بررسی مدل	- تعیین محدوده کیفیت - تحلیل امنیت و مخاطره حریم خصوصی	- آموزش متمرکز

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.

شکل الف-۲- تطابق فرایند توسعه نرم‌افزاری با چارچوب الزامی سازمان

کلید کلمات کوته‌نوشت

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	بازبینی نهایی امنیت

الف-۴ زمینه کسب‌وکار

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

الف- مدیریت توسعه پروژه، تحلیل مخاطره، فرایندهای عملیاتی، ممیزی و واپایش فرایندها

ب- خط‌مشی امنیتی سازمان

پ- شیوه نوین برای زمینه کسب‌وکار

ت- توسعه روش‌های مورداستفاده توسط سازمان

ث- بیان بهترین شیوه‌ها برای کاربردهای مورداستفاده توسط سازمان در زمینه فناوری

ج- فرایند مدیریت پروژه‌ای رسمی سازمان

چ- پذیرش سایر استانداردهای بین‌المللی مرتبط با استاندارد ملی ISO/IEC مانند استانداردهایی هم‌چون، استاندارد ملی ایران به شماره ۲۷۰۰۱ : سال ۱۳۸۷، استاندارد ملی ایران به شماره ۲۷۰۰۲ : سال ۱۳۸۷و ISO/IEC 15288.

زمینه کسب‌وکار به‌وسیله ترکیبی از خط‌مشی‌های شرکت‌های بزرگ، خط‌مشی‌های منطقه‌ای خاص، زمینه فنی و فناوری و حضور بازار در واحدهای کسب‌وکار 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 واپایش 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 روش-های توسعه یا ابزارها امکان‌پذیر نیست. بنابراین گروه‌های کسب‌وکار مجاز به مقابله با چالش‌های فنی هستند که مستقیماً توسط خط‌مشی چرخه توسعه امنیت تحت پوشش قرار نمی‌گیرند.(که این موارد با جزئیات بیشتر در نقش‌ها، مسئولیت‌ها و بخش مدارک زیر مشخص‌شده است.)

الف-۵ زمینه مقرراتی

بند ۸-۱-۲-۲ موارد چارچوب نظارتی و اسناد مرتبط با قوانین یا مقررات در هر یک از مکان‌های کسب‌وکار 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 توسعه‌یافته‌اند یا مستقرشده‌اند یا مورداستفاده 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 جغراسیاسی[1] توسط فرایندهای کسب‌وکار موجود پوشش داده می‌شود و فعالانه برای اطلاع‌رسانی به فعالیت‌های طراحی و توسعه گروه‌های پروژه مورداستفاده قرار می-گیرد.

خط‌مشی‌ها به‌وسیله واحدهای کسب‌وکار و امور حقوقی مورد تحلیل قرار می‌گیرند. برای اطمینان از این‌که تمام جنبه‌های ایجاد و انتشار برنامه‌های کاربردی با معیارهای شناخته‌شده حقوقی و قانونی در مناطق مختلف روبرو می‌شوند و هر پروژه جدید بر اساس چارچوب خط‌مشی‌های موجود عمل می‌کند.

برخی از برنامه‌های کاربردی (همراه با موارد ذکرشده در بالا)، به‌وسیله گروه‌های محصول استفاده می‌شوند که به‌طور خودکار فرایند تضمین تطابق مقررات را برای نرم‌افزارهای کاربردی و استفاده عمومی توسعه می‌دهند. درنهایت، 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. بااین‌حال مهم است توجه کنیم که خط‌مشی‌های نظارتی و جغراسیاسی به‌وسیله چرخه توسعه امنیت تعیین نمی‌شوند.

الف-۶ انباره مشخصات برنامه کاربردی

1 - Geopolitical

بند ۸-۱-۲-۳ انباره مشخصات برنامه کاربردی، نیازهای کارکردی کلی فناوری و راه‌حل‌های از پیش تأییدشده مطابق با آن‌ها را فهرست و ثبت می‌کند. توصیه می‌شود مشخصات برنامه شامل موارد زیر باشد:

الف- محاسبه ویژگی‌های کاربردی، ذخیره‌سازی و انتقال اطلاعات

ب- پارامترهای معمول، برنامه، ویژگی‌ها، خدمات و نیازها

پ- کد منبع، کد دودویی، محصولات یا خدمات استفاده‌شده یا متکی به برنامه‌های کاربردی

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

الف- سامانه‌های دیگر

ب- زمان مؤلفه‌های زیرساخت‌ها که بستگی به عوامل متعددی دارد.

پ- فهرست واپایش در محیط و زمان اجرا

مشخصات به‌وسیله واحدهای کسب‌وکار فردی نوشته و ذخیره می‌شوند و به‌طورکلی شامل دو راهنمای عملکردی(تعیین این‌که توصیه می‌شود، چگونه یک مؤلفه خاص اطلاعات را محاسبه، ذخیره و انتقال یابد) و راهنمای فنی (تعیین زبان‌های برنامه‌نویسی، مترجم‌ها، کتابخانه‌ها و...) می‌شوند.

در برخی موارد، چرخه توسعه امنیت، خط‌مشی‌هایی را برای مؤلفه‌ها 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 نیازهای کارکردی یا تسهیلات نباید در معرض خطر قرار گیرد.

الف-۷ زمینه فناوری

۸-۱-۲-۴ 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 افزاره‌های فنی است.

مثال – زمینه‌های فناوری که ممکن است تأثیر 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 کسب‌وکار 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 کسب‌وکار و زمینه فناوری که به‌طور مستقل به‌وسیله هر واحد تجاری تنظیم می‌شود، به آن‌ها اجازه رفع نیازهای خود را می‌دهد. بااین‌حال واحدهای کسب‌وکار همچنین توصیه می‌شود اطمینان دهند که پروژه‌های نرم‌افزاری از خدمات فناوری اطلاعات استفاده می‌کنند و فناوری به آن‌ها اجازه می‌دهد معیارهای امنیتی داشته باشند که در زمینه کسب‌وکار و نظارت تنظیم می‌شوند.

الف-۸ نقش‌ها، مسئولیت‌ها و صلاحیت‌ها

۸-۱-۲-۵ توصیه می‌شود ONF حاوی موارد زیر شود:

الف- فهرست و شرح همه نقش‌ها، مسئولیت‌ها و صلاحیت‌های حرفه‌ای موردنیاز برای افراد درگیر در ایجاد و حفظ چارچوب و نقش‌های مختلف برای ایجاد و حفظ کاربرد واپایش‌های امنیتی

ب- فهرست و شرح همه نقش‌ها، مسئولیت‌ها و صلاحیت‌های حرفه‌ای موردنیاز برای افراد درگیر در برنامه کاربردی سازمان مثل مدیریت امنیت اطلاعات، مدیران پروژه، مدیران راهبر، تحصیل نرم‌افزار، مدیران توسعه نرم‌افزار، صاحبان برنامه‌های کاربردی، مدیران کاربر، معماران، برنامه نویسان، آزمون‌گران، مدیران سامانه، دادگان مدیران، مدیران شبکه و کارکنان فنی.

این‌یک خط‌مشی گسترده‌سازمانی است که اطمینان می‌دهد تمام نقش‌های حیاتی برای تمام مراحل مشخص‌شده‌اند ، تمام مسئولیت‌ها تعریف‌شده‌اند 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 کسب‌وکار ایجاد و نگهداری می‌شوند. این گروه‌ها شامل توصیف سطوح بالای وظایف و صلاحیت‌های منحصربه‌فرد برای هر نقش شغلی هستند. درحالی‌که منابع انسانی شرح برخی از مشاغل را حفظ می‌کنند ولی عموماً واحدهای کسب‌وکار 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 گروه توسعه خواهد بود.

فرایند توسعه نرم‌افزار، دارای معیارهای عمومی و شرح کار برای نقش‌های امنیتی و خصوصی است، این نقش‌ها در طی مراحل موردنیاز برای فرایند توسعه نرم‌افزار اختصاص داده می‌شوند. توصیه می‌شود نقش‌های ویژه شغلی 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 عبارت‌اند از:

نقش‌های نظارتی: این نقش‌ها جهت ارائه نظارت بر پروژه طراحی شدند و ممکن است شامل مشاوره کمی و کیفی به گروه‌های پروژه جهت ایجاد یک کمینه اطمینان قابل‌قبول و ایجاد آستانه اطمینان برای یک پروژه کاربردی باشند. توصیه می‌شود نقش‌های نظارتی به مقامات ذی‌صلاح جهت پذیرش یا رد امنیت و حفظ حریم خصوصی برنامه‌ها واگذار شوند. در یک پروژه گروهی:

الف- مشاور امنیتی: این نقش توسط افرادی با تخصص امنیت فردی از بیرون از افراد گروه 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. توصیه می‌شود شخص انتخاب‌شده برای این وظیفه دو نقش فرعی زیر را ایفا کند:

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

۲- کارشناس: توصیه می‌شود فرد انتخاب‌شده برای نقش مشاور امنیتی موضوعات قابل‌تأییدی با تخصص در امنیت در اختیار بگذارد.

ب- مشاور در زمینه مسائل خصوصی: این نقش توسط کارشناس مسائل خصوصی و فردی از بیرون از گروه 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. توصیه می‌شود فردی که برای این وظیفه انتخاب می‌شود، دو نقش فرعی زیر را ایفا کند:

۱- ممیز: توصیه می‌شود این فرد بر رویه توسعه حریم خصوصی نظارت کند و بر پایان موفقیت‌آمیز هر مرحله موردنیاز گواهی دهد. توصیه می‌شود مشاور در این زمینه آگاهی کافی جهت گواهی دادن بر انطباق یا عدم انطباق با نیازهای خصوصی بدون وجود دخالتی از گروه‌های پروژه داشته باشد.

۲- خبره: توصیه می‌شود فرد انتخاب‌شده برای نقش مشاور در زمینه حریم خصوصی تخصص قابل‌تأیید 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 بامهارت و تجربه مناسب را می‌توان شناسایی کرد.

نقش‌های اصلی گروه: توصیه می‌شود نقش‌های اصلی گروه توسط خبرگانی اتخاذ شود که پروژه گروه‌های توسعه را در بحث و مذاکره با مشاوران امنیت و حفظ حریم خصوصی ارائه می‌کنند. این نقش مسئول مذاکره، پذیرش و ردیابی کمینه نیازهای امنیتی، حفظ خطوط روشنی از ارتباط با مشاوران و سایر تصمیم‌گیرندگان در طول مدت پروژه توسعه نرم‌افزار است.

الف- راهنمای گروه امنیت: این فرد (یا گروهی از افراد)، مسئولیتی ازاین‌جهت که تضمین کند انتشار نرم-افزار، تعیین‌کننده تمام موضوعات امنیتی است را ندارند. بااین‌حال، 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 گروه پروژه است.

ب- راهنمای گروه حریم خصوصی: این فرد (یا گروهی از افراد)، مسئولیتی ازاین‌جهت که تضمین کند انتشار نرم‌افزار، تعیین‌کننده تمام موضوعات حریم خصوصی است را ندارد. بااین‌حال، 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 (به‌عنوان‌مثال راهنمای توسعه و ...) در گروه پروژه است.

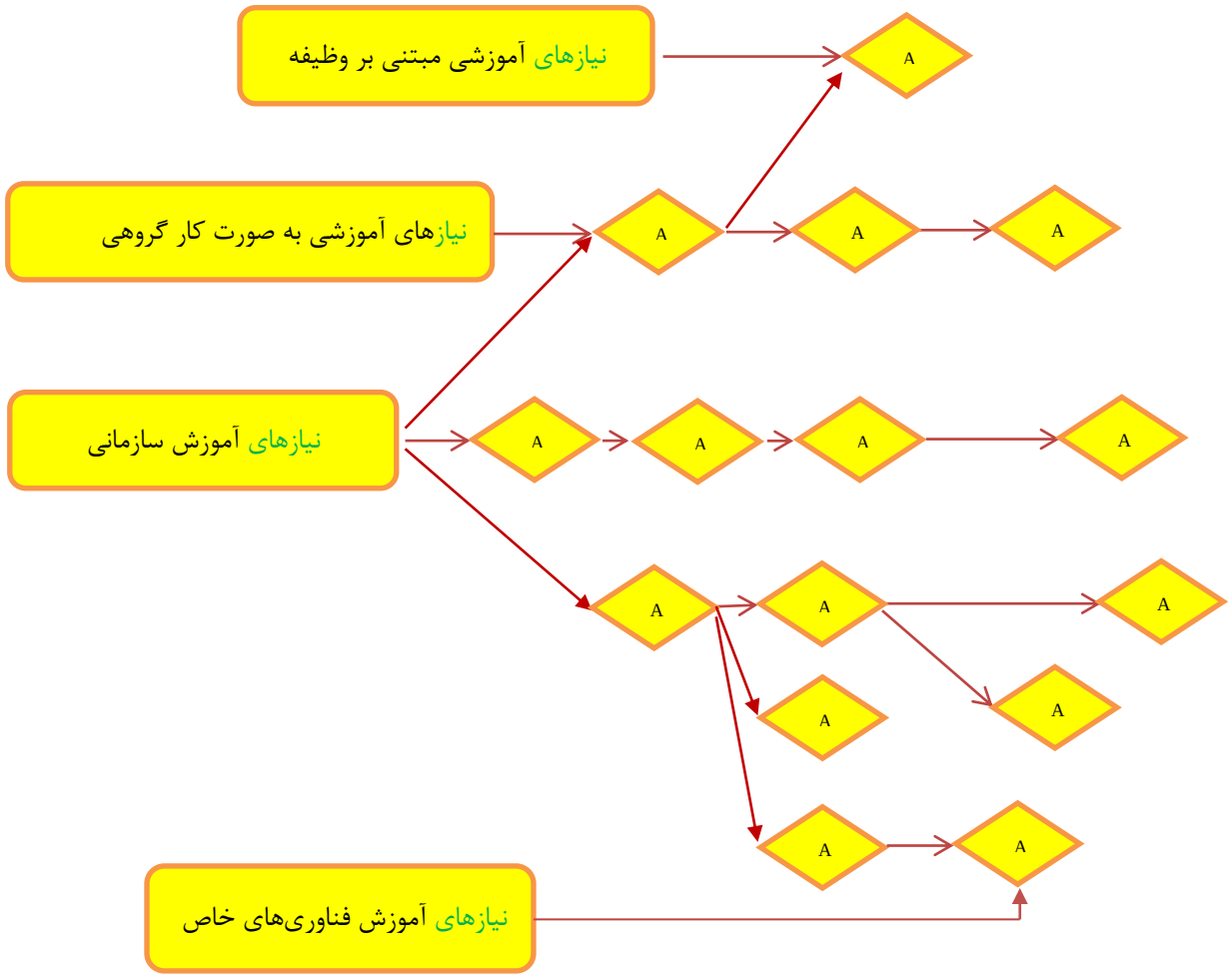
الف-۹ کتابخانه ASC سازمان

۸-۱-۲-۶ توصیه می‌شود سازمان کمینه یک کتابخانه واپایشی برای کاربردهای امنیتی داشته باشد. این کتابخانه، کتابخانه واپایش برنامه کاربردی نامیده می‌شود که تمامی ASCهای شناخته‌شده توسط سازمان را فهرست و مستندسازی می‌کند. این واپایشASCها، از استانداردها، به‌روش‌ها و نقش‌ها،

مسئولیت‌ها و مدارک حرفه‌ای، فناوری، کسب‌وکار و زمینه‌های نظارتی و مشخصات برنامه‌های کاربردی تکامل‌یافته است.

هفده واپایشASC، به‌عنوان قسمتی از فرایند توسعه نرم‌افزار که در زیر توصیف‌شده ، شناسایی‌شده‌اند. این مثال شامل هر دو وظایف اجباری و اختیاری می‌شود. آن بخش از وظایف واپایش امنیتی برنامه کاربردی که الزامی نیستند، ممکن است در صورت لزوم توسط واحدهای کسب‌وکار در راستای رسیدن به اهداف مطلوب امنیتی و اهداف حریم خصوصی، توسعه یابند. کتابخانه کاربردی واپایش امنیتی که در زیر ترسیم می‌شود از روش‌های سنتی توسعه استفاده می‌کند. به خاطر حفظ ایجاز و ارائه مفید مطالب بخش‌های مازاد تحت واپایش امنیتی برنامه کاربردی حذف‌شده است.

سمت چپ در واپایش امنیتی برنامه کاربردی ذیل، به‌عنوان ASC «ریشه» در نظر گرفته می‌شود که درواقع «نقطه والد» از درخت ASC است که با جزئیات در شکل زیر نشان داده‌شده است. این شکل فرضی نشان می‌دهد که ASC به‌وسیله سازمانی با سطوح فزاینده پیچیدگی و جزئیات به کار می‌رود تا به حد اعتماد موردنظر 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- **نیازهای آموزش**: توصیه می‌شود همه اعضای گروه توسعه نرم‌افزاری 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، توصیه می‌شود دست کم در یک کلاس آموزشی امنیتی در هرسال شرکت کنند.

توصیه می‌شود آموزش پایه‌ای امنیت نرم‌افزار، مفاهیم بنیادی مانند طراحی امن، مدل‌سازی تهدید، سنجش میزان سطوح نفوذ، برنامه‌نویسی امن، آزمون امنیتی و مسائل خصوصی.

الف-۹-۲ نیازها

۲-نیازهای 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 نیازهای یک برنامه کاربردی در طی مراحل برنامه‌ریزی اولیه یک مسئله جدید و مهم است. این به گروه‌های 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 کمینه برساند.

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

۳- دروازه‌های کیفیت/نوارهای اشکال[1]: 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 گروه‌ها را قادر می‌سازد امنیت و نقصان‌های آن را در طی مسیر توسعه، شناسایی و تصحیح کنند. توصیه می‌شود یک پروژه گروهی 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 نیازهای امنیتی شدیدی پذیرفته می‌شود.

همچنین توصیه می‌شود گروه پروژه انطباق با مذاکراتی که در محدوده کیفیت انجام شد و در جهت تطابق با نیازهای 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.

یادآوری- مفهوم دروازه‌های کیفیت/نوارهای اشکال که در امنیت به کار بسته‌شده است، نزدیک به مفهوم سطح اطمینان هدف-گذاری شده است، زیرا برای برقراری کمترین سطوح قابل‌قبول از امنیت و حریم خصوصی به‌کاربرده می‌شود.

1- Bug Bar

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. توصیه می‌شود چنین ارزیابی‌هایی 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 گروه موردنظر ما هستند، دارد؟ هر بخش پروژه که نیاز به آزمون دارد باید مسائل شناسایی‌شده توسط اعضای این گروه را قبل از این‌که پروژه جهت انتشار آماده تصویب شود، حل کند.

ت- (امنیت) هر آزمون دیگر یا تحلیل نیازهای امنیتی توسط مشاور امنیتی که جهت کاهش مخاطره امنیتی لازم است، باید انجام شود.

ث- (امنیت) تعیین محدوده خاص موردنیاز از آزمون fuzz (در زیر قسمت ASC/12)

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. (به‌عنوان‌مثال کاربر بر روی یک پیونده خاص کلیک می‌کند و به یک وبگاه 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 شناسایی‌شده‌ای در ماشین ذخیره نمی‌گردد. هیچ تنظیماتی در طرف کاربر تغییر نمی‌کند و هیچ نرم‌افزاری نصب نمی‌شود.

الف-۹-۳ طراحی

۵-نیازهای طراحی: زمان بهینه برای تأثیرگذاری در طراحی قابل‌اعتماد برای یک پروژه در چرخه عمر آن است. این بسیار مهم است که نگرانی‌های امنیتی و حریم خصوصی به‌دقت 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. توصیه می‌شود گروه‌های پروژه 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 گروه پروژه مهم است که تمایز بین امنیت ویژگی‌ها یا ویژگی‌های امنیتی را درک کنند. ادراک این مفاهیم، پیاده‌سازی امنیت ویژگی‌ها که درواقع غیرمطمئن هستند را امکان‌پذیر می‌سازد.

ویژگی‌های امنیتی این‌گونه تعریف می‌شوند: ویژگی‌هایی که ازنظر عملکردی با توجه به مسائل امنیتی به‌خوبی طراحی‌شده‌اند 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.

درنتیجه، توصیه می‌شود تمام مشخصات طرح موردنظر:

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

ب- چگونگی پیاده‌سازی امن تمام قابلیت‌ها توسط یکی از ویژگی‌های موردنظر توصیف کند

پ- چگونگی استقرار ویژگی‌ها را به طور امن توصیف کند

نیازهای طراحی شامل تعدادی از اقدامات موردنیاز است که شامل اما محدود به بررسی طرح امنیت، حریم خصوصی، مشخصات آن و پیاده‌سازی کمینه رمزنگاشتی موردنیاز طراحی است.

۶- کاهش سطحی حمله: کاهش سطح حمله با مدل‌سازی تهدید همسو است، 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 نقطه‌ضعف یا آسیب‌پذیری احتمال و شانس کمتری می‌دهد.

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

۷- مدل‌سازی تهدید: مدل‌سازی تهدید، یک فرایند الزامی انجام‌شده در مرحله طراحی است که به گروه‌های 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 گروهی است که شامل مؤلفه‌هایی 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: توصیه می‌شود تمامی گروه‌های توسعه فهرستی از ابزارهای تأییدشده (قابلیت‌های امنیتی خاص مانند مترجم‌ها و ...) را برای استفاده در برنامه‌های نرم‌افزاری تعریف کرده و انتشار دهند. توصیه می‌شود این فهرست توسط مشاور امنیتی برای اعضای گروه پروژه شناسایی و تأیید می‌شود. به‌طورکلی، توصیه می‌شود گروه‌های توسعه تلاش کنند جهت استفاده از آخرین نسخه ابزارهای مصوب از قابلیت‌های امنیتی جدید منتفع شوند.

۹- کارکردهای منسوخ[1] ناامن: بسیاری از کارکردهای مورداستفاده و رایج و برنامه‌های کاربردی، در مواجهه با گروه‌های پروژه تهدیدات زیست‌محیطی امن نیستند و توصیه می‌شود تحلیل شوند. تمام کارکردها و واسط-های برنامه نویسی کاربردی (API) [2] که در ارتباط با پروژه توسعه نرم‌افزار مورداستفاده قرار خواهد گرفت و مانع از آن شود که امنیت کافی را نداشته باشد.

پس‌ازآنکه این فهرست خودداری تهیه شد، توصیه می‌شود گروه‌های پروژه از فایل‌ها، مترجم‌های جدیدتر یا ابزارهای پویش کد مخصوص چک کردن آن، برای اعتماد از عدم استفاده از برنامه‌های کارکردی خودداری شده و جایگزینی آن با موارد دارای امنیت بیشتر استفاده کنند.

۱۰- تحلیل ایستا: توصیه می‌شود گروه پروژه تحلیل کد ایستا از کد منبع را انجام دهند. تحلیل ایستا از کد منبع یک‌راه حل قیاس پذیر برای بررسی کد امنیتی فراهم می‌کند و می‌تواند مورداستفاده قرار گیرد و اعتماد دهد که منجر به خط‌مشی‌های کدگذاری امنیتی تنظیم‌شده توسط گروه امنیتی می‌شود و پیشروی مشاور امنیتی قرار می‌گیرد.

تحلیل کد ایستا به‌خودی‌خود، عموماً ناکافی است. برای انجام بررسی‌های امنیتی کامل، گروه امنیتی و مشاوران امنیتی باید از نقاط ضعف و قوت ابزارهای تحلیل ایستا 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 به‌موقع کد، با استفاده از تحلیل کارکرد رخ می‌دهد. سایر کارکردهای تحلیل ایستا در مواقع لزوم انجام می‌گیرد.

الف-۹-۵ درستی‌سنجی

۱۱- تحلیل برنامه پویا: درستی‌سنجی زمان اجرای برنامه‌های نرم‌افزاری ضرورت دارد تا اطمینان حاصل شود که قابلیت یک برنامه نرم‌افزاری مانند آنچه طرح‌ریزی‌شده هست. توصیه می‌شود این وظیفه درستی‌سنجی، ابزارهایی را که رفتار برنامه کاربردی را از جهت نداشتن ضعف، استفاده از امتیاز مسائل یا سایر موضوعات انتقادی امنیتی پایش می‌کند، مشخص سازد. فرایند توسعه نرم‌افزار از ابزارهای مبتنی بر زمان اجرا به همراه سایر فناوری‌ها مانند آزمون fuzz برای دست یافتن به سطوح مطلوب پوشش آزمون امنیتی استفاده می‌کند.

۱۲- آزمون fuzz: این آزمون جهت رفع مشکلات برنامه به‌وسیله شناسایی نقص برنامه‌ها یا بررسی استفاده از داده‌های تصادفی به‌عنوان ورودی برنامه‌ها استفاده می‌شود. چرخه توسعه، نرم‌افزار آزمون fuzz انجام‌شده بر روی برنامه‌های متعدد و موارد مشابه آن را مشخص می‌کند. این آزمون ازنظر کارکردی در برنامه‌های کاربردی موردنظر و مشخصات موردتوجه کارکردی و فنی برای نرم‌افزارهای کاربردی استفاده می‌شود. مشاور امنیتی ممکن است نیاز به آزمون‌های fuzz بیشتر یا افزایش دامنه و مدت این آزمون را بر اساس کارکرد برنامه کاربردی موردنظر لازم بداند.

۱۳- بررسی مدل تهدید/ تهدید سطحی: این بررسی برای یک برنامه کاربردی که انحراف قابل‌توجهی از مشخصات کارکردی و فنی ایجادشده در طول مسیر طراحی یک پروژه توسعه نرم‌افزار دارد، رایج است. بنابراین

1 - Depricate
2 - Application Porgramming Interface

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 گرفته‌شده و تعدیل می‌شود.

۱۴- بازبینی کد راهنما (اختیاری) : بازبینی کد راهنما به‌عنوان یک وظیفه اختیاری در چرخه توسعه نرم‌افزار تلقی می‌شود. بررسی این کد، معمولاً توسط اعضای گروه امنیت کاربردی با توجه به توصیه مشاوران امنیتی انجام می‌شود. درحالی‌که ابزارهای تحلیل می‌توانند کار شناسایی ضعف‌ها یا آسیب‌پذیری‌ها را انجام دهند، اما کامل نیستند. بررسی کد راهنما معمولاً بر مؤلفه‌های بحرانی یک کاربرد تمرکز می‌کند و اغلب درجایی که داده-های حساس مانند اطلاعات شناسایی شخص درگیر می‌شوند، مورداستفاده قرار می‌گیرد. این راهنما همچنین در بررسی‌های سایر مؤلفه‌های حساس استفاده می‌شود.

الف-۹-۶ انتشار

۱۵- طرح پاسخ به رخداد: موضوع گشایش و انتشار هر نرم‌افزاری که از نیازهای چرخه توسعه نرم‌افزاری است، باید شامل یک طرح واکنش به مسائل باشد. هر برنامه‌ای حتی بدون آسیب‌پذیری‌های شناخته‌شده در زمان گشایش، می‌تواند موضوع تهدیداتی باشد که باگذشت زمان پدیدار می‌شود. توصیه می‌شود طرح پاسخ به رخداد شامل موارد زیر به‌صورت کمینه است:

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

ب- ارتباط تلفنی با مجوز تصمیم‌گیرندگی به‌صورت شبانه‌روزی (۲۴*۷*۳۶۵)

پ- طرح خدمات امنیتی برای کدهای به‌جامانده 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- بازبینی امنیتی نهایی (FSR)[1]: این بازبینی شامل بررسی دقیق از تمام فعالیت‌های امنیتی انجام‌شده، بر اساس برنامه‌های کاربردی نرم‌افزار، قبل از انتشار آن است. این بازبینی امنیتی نهایی توسط مشاور امنیتی با کمک کارکنان منظم بخش توسعه و هدایت گروه امنیتی و حفظ حریم خصوصی انجام می‌شود. بازبینی FSR یک بازبینی ساده نیست، درواقع فرصتی برای انجام فعالیت‌های امنیتی است که قبلاً نادیده گرفته‌شده یا فراموش‌شده‌اند. بازبینی FSR معمولاً شامل بررسی مدل‌های تهدید، بررسی درخواست‌های استثنا ، بررسی ابزار و کارکرد ازنظر کیفیت مشخص‌شده قبلی است. این بازبینی امنیتی نهایی ، سه نتیجه متفاوت خواهد داشت:

1- Final Security Review

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

ب- **بازبینی امنیتی نهایی گذرانده شده با استثناء:** تمام موضوعات امنیتی و حریم خصوصی که توسط این فرایند بررسی می‌شوند، ثابت هستند و بررسی‌هایی که نمی‌توانند به‌درستی تعیین شوند ، اصلاح‌شده و در نسخه تصحیح‌شده بعدی وارد سامانه می‌شوند.

پ- **بازبینی امنیتی نهایی به‌صورت مداوم:** اگر یک گروه با تمام نیازهای چرخه توسعه نرم‌افزار مواجه نباشند و مشاور امنیتی و گروه تولید نتوانند به مصالح قابل‌قبول دسترسی یابند، مشاور امنیتی نمی‌تواند پروژه را تأیید کند و این پروژه نمی‌تواند انتشار یابد. گروه‌ها باید کلیه نیازهای چرخه توسعه نرم‌افزار را تعیین کنند مبنی بر این‌که می‌توانند آن را راه‌اندازی کرده یا مدیران اجرایی را مجبور به تصمیم‌گیری در این زمینه کنند.

یادآوری- نتایج FSR به مفهوم سطح واقعی اعتماد نزدیک است چنانچه FSR بررسی آزمون تمامی عملکرد فعالیت‌های امنیت بر روی نرم‌افزار 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 اختصاص‌یافته برای هر فرایند انتشار، توصیه می‌شود تضمین کند که گروه پروژه نیازهای امنیتی رضایت بخشی دارد. مشاور امنیت باید برای گروه پروژه که تمامی نیازها را برآورده می‌سازد، اختصاص داده شود.به‌طور مشابه برای تمامی محصولات که کمینه دارای یک مؤلفه با نرخ اثر حریم خصوصی P1 باشند، مشاور حریم خصوصی پروژه باید تأیید کند که گروه پروژه تمامی نیازهای حریم خصوصی قبل از اینکه اجرا شود را برآورده سازد.

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

الف-۱۰ ممیزی امنیت برنامه کاربردی

۸-۵-۱ هدف پنجمین گام از ASMP درستی‌سنجی و ضبط رسمی شواهد پشتیبانی که آیا برنامه کاربردی خاص به‌دست‌آمده 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. بر اساس 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 قابل‌پذیرش باشد، انجام دهد.

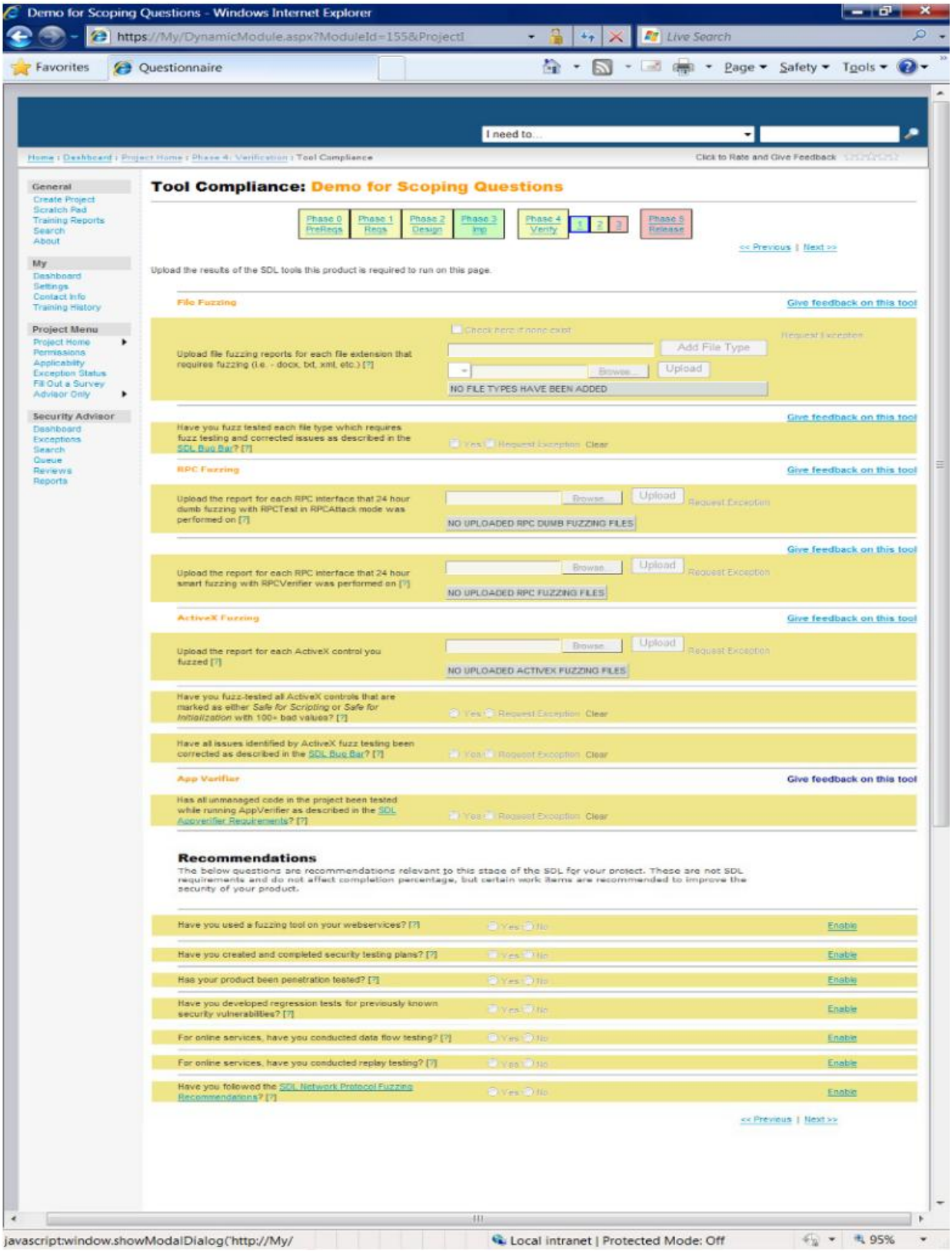
مثال۳: یک سازمان می‌تواند، این گام را در طی مراحل عملیاتی یک برنامه کاربردی چرخه حیات به‌عنوان بخشی از ممیزی امنیتی سالیانه سازمان انجام دهد.

در این مرحله، گروه داخلی یا خارجی (بر اساس خط‌مشی‌های سازمانی موجود) و ساختار اصلی سازمان تأیید می‌کند که تمام سنجش‌های فراهم‌شده به‌وسیله کاربرد واپایش‌های امنیتی برای یک کاربرد ویژه، انجام و نتایج آن تأییدشده است. هدف این گام اثبات سطح واقعی امنیت کاربردی در یک‌زمان 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 نرم‌افزار، در برمی‌گیرد.

- طراحی ویژه‌ای از برنامه‌های کاربردی کسب‌وکار جهت پیگیری مطابقت با برنامه توسعه نرم‌افزار و ابزارهای مورداستفاده مدل‌های تهدید استفاده می‌شود و سایر شواهد خودکار و غیر خودکار ذخیره می‌شوند.
- راهبران گروه‌های امنیتی و حفظ حریم خصوصی باید اطمینان بدهند که اطلاعات لازم برای بررسی موضوعی جمع‌آوری‌شده و ازنظر برنامه کاربردی مورد پیگیری قرار گرفتند.
- این اطلاعات که ازنظر کاربردی موردبررسی قرار گرفتند، به‌وسیله مشاوران امنیتی و حفظ حریم خصوصی جهت فراهم کردن یک چارچوب برای بررسی امنیتی نهایی(بر اساس مطالب فوق‌الذکر)، استفاده می‌شوند.
- مشاوران امنیتی و حفظ حریم خصوصی مسئول بررسی اطلاعات واردشده و پیگیری کاربردی بودن آن (که این شامل بررسی نهایی امنیتی و سایر وظایف امنیتی طرح‌ریزی‌شده توسط مشاوران می‌شود.) و اطمینان از این‌که تمام نیازمندی‌ها و انتظارات حل‌شده، هستند.

عکس تهیه شده از برنامه کاربردی استفاده‌شده برای ردیابی و درستی سنجی وظایف امنیت در شکل الف-۴ نشان داده شده است.



شکل الف-۴- مثالی از یک برنامه کاربردی کسب‌وکار برای ممیزی امنیت برنامه کابردی

الف-۱۱ مدل چرخه حیات برنامه کاربردی

۸-۱-۲-۷-۱ سازمانی که کسب‌وکارش 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 بر اساس زمینه موردبررسی 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 منحصربه‌فرد و سفارشی است که اغلب برای زمان‌های متعدد در حال استفاده بوده و در طی سال‌ها اصلاح‌شده است. این مدل به‌عنوان 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 شکل‌گرفته‌اند 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، کسب‌وکار و نظارتی و نقشی که در هر یک از زمینه‌ها ایفا می‌شود را طرح‌ریزی می‌کنند.

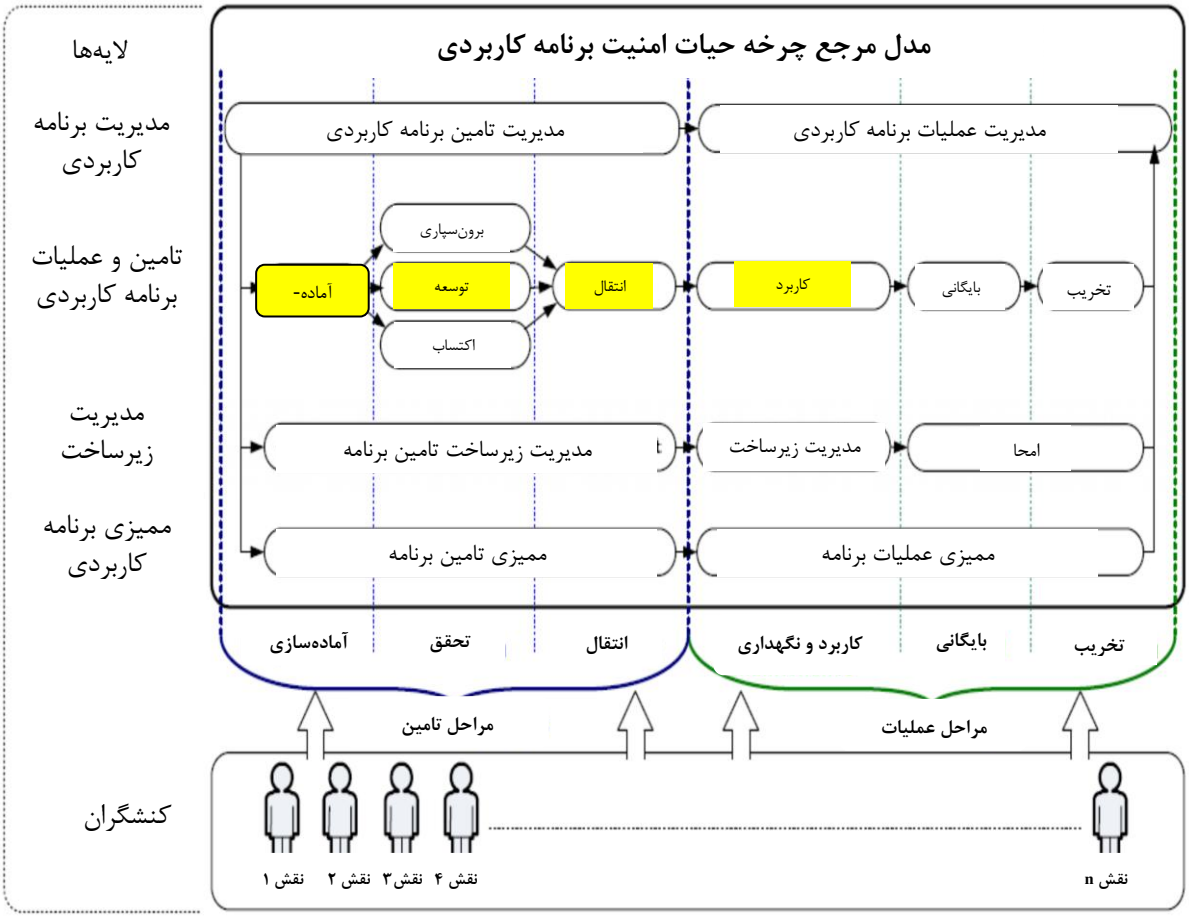
یک تصویر ساده از فرایند توسعه نرم‌افزار در شکل الف-۵ نمایش داده‌شده است. این نمودار مشاهده کاربرد واپایش‌های امنیتی مورداستفاده در یک پروژه فرضی از آموزش کارکنان تا مرحله انتشار برنامه‌های کاربردی در یک پروژه فرضی است. این‌یک نمودار جامع نیست، همان‌طور که قبلاً اشاره شد، بسیاری از گروه‌ها سایر وظایف امنیتی و خصوصی را که مختص برنامه‌های خاص خودشان است را به آن می‌افزایند.

شکل الف-۵- نمایشی از فرایند SDL (فلش آبی: نه – فلش قرمز: بله)

الف-۱۲ طرح فرایند توسعه نرم‌افزار بر اساس مدل مرجع چرخه حیات امنیت

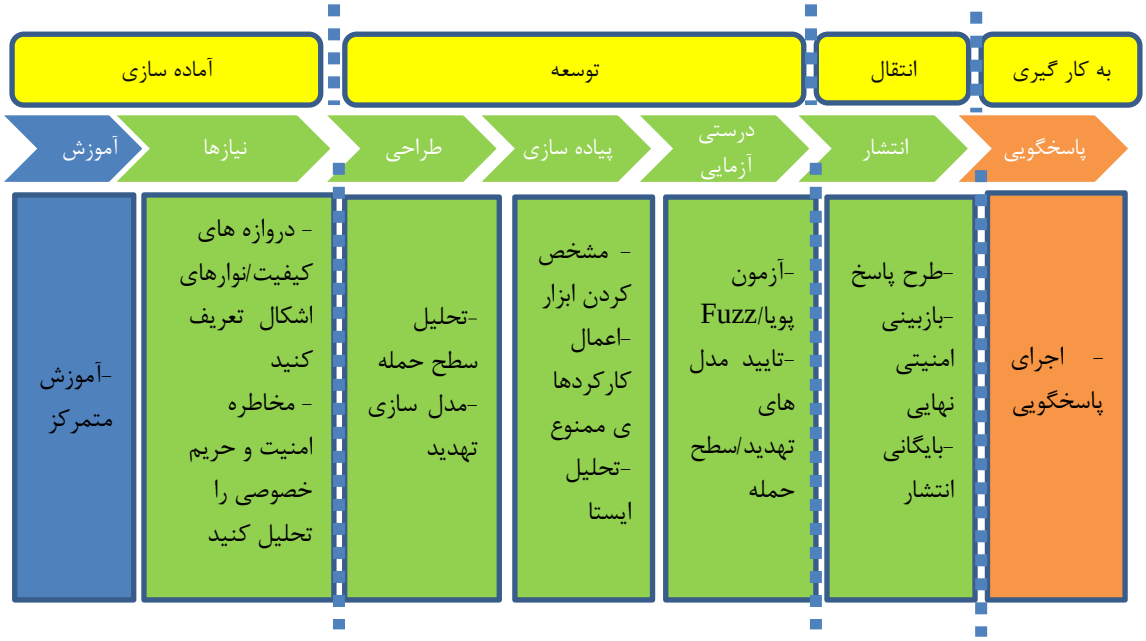
فرایند توسعه نرم‌افزار می‌تواند بر اساس مدل مرجع چرخه حیات امنیت برنامه کاربردی که شامل استاندارد ISO/IEC 27034 می‌شود، طرح‌ریزی شود. مراحل مدل مرجع توسط فرایند توسعه برنامه کاربردی که به شکل پررنگ شده در شکل الف-۶ نمایش داده‌شده ، پوشش داده می‌شود:

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



شکل الف-۶- نگاشت فرایند توسعه نرم‌افزار مطابق با چرخه حیات امنیت برنامه کاربردی

به‌علاوه، شکل الف-۷ جزئیات بیشتری از طرح مراحل فرایند توسعه نرم‌افزار را بر اساس مراحل کاربرد مدل مرجع چرخه حیات نشان می‌دهد.



شکل الف-۷- نگاشت با جزییات مراحل فرایند توسعه نرم‌افزار با مراحل کاربرد امنیت چرخه حیات مدل مرجع

مراجع پیوست الف

زمینه کسب‌وکار

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

واپایش کتابخانه ASC سازمان

آموزش

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

نیازها

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

پیاده‌سازی

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 واپایش ASC با یک استاندارد موجود

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

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

ب-۱ طبقه‌بندی‌های نامزد برنامه کاربرد واپایش‌های امنیت

این بند تلاش می‌کند جنبه‌های احتمالی طبقه‌بندی‌های نامزد کاربرد واپایش‌های امنیتی را که به‌طور مستقیم از SP-800-53 نقل‌شده 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 واپایش‌های امنیت رایج

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

ب-۱-۲ ملاحظات مرتبط عملیاتی / محیطی

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

ب-۱-۳ ملاحظات مرتبط با زیرساخت فیزیکی

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

ب-۱-۴ ملاحظات مرتبط با دسترسی عمومی

ازآنجایی‌که ممکن است برخی واپایش‌های امنیتی از پایه‌های خاص واپایشی (به‌عنوان‌مثال شناسایی، احراز هویت و واپایش امنیتی کارکنان) برای کاربرانی که از طریق رابط‌های عمومی به سامانه‌های اطلاعاتی دسترسی پیدا می‌کنند، قابل‌اجرا نباشند، واپایش‌های امنیتی مرتبط با دسترسی عمومی به سامانه‌های اطلاعاتی باید به‌دقت در نظر گرفته شوند و ملاحظات لازم در آن به کار گرفته شود. برای مثال درحالی‌که واپایش‌های پایه‌ای شناسایی و احراز هویت کارکنان سازمانی که از سامانه‌های اطلاعاتی تامین‌کننده خدمات دسترسی همگانی حفاظت و پشتیبانی می‌کنند را لازم می‌داند، ممکن است همین واپایش‌ها برای دسترسی به سامانه‌های اطلاعاتی از طریق رابط‌های همگانی و به‌منظور اکتساب 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

واپایش‌های امنیتی مربوط به فناوری‌های خاص(به‌عنوان‌مثال بی‌سیم، رمزنگاری، واپایش‌های عمومی امنیتی و زیرساخت‌های کلیدی عمومی) قابل‌اجرا هستند، تنها اگر این فناوری‌ها برای به‌کارگیری در سامانه اطلاعاتی به کار گرفته شوند یا موردنیاز باشند.

واپایش‌های امنیتی تنها در سامانه‌های اطلاعاتی که از قابلیت‌های امنیتی تعیین‌شده به‌وسیله واپایش یا منبع کاهش تهدید بالقوه به‌وسیله واپایش استفاده می‌کنند، قابل‌اجرا هستند. به‌عنوان‌مثال وقتی مؤلفه‌های یک سامانه تک کاربردی هستند، شبکه‌ای نبوده یا فقط مختص شبکه‌های محلی‌اند، یک یا بیش از یک ویژگی منطق کافی برای عدم پذیرش واپایش‌های انتخاب‌شده توسط مؤلفه‌ها فراهم می‌کنند.

واپایش‌های امنیتی که می‌توانند به‌صراحت یا به‌طور ضمنی توسط سازوکارهای خودکار حمایت شوند، درصورتی‌که سازوکاری وجود نداشته باشد یا به‌آسانی در محصولات تجاری یا دولتی در دسترس نباشد، نیاز به توسعه این‌چنین سازوکارهایی ندارند. در شرایطی که سازوکارهای خودکار به‌راحتی در دسترس نباشند، مقرون‌به‌صرفه نبوده و یا ازنظر فنی امکان‌پذیر نباشد؛ جبران واپایش‌های امنیتی از طریق اجرای سازوکارهای غیر خودکار یا روش‌هایی جهت برآوردن واپایش‌های امنیتی یا پیشرفت‌های واپایشی باید انجام شود.(شرایط و ضوابط استفاده از واپایش‌های جبرانی در زیر را ملاحظه فرمایید.)

ب-۱-۶ ملاحظات سیاسی / نظارتی

واپایش‌های امنیتی که موضوعاتی را به‌وسیله قوانین قابل‌اجرا، دستورات اجرای دستورالعمل‌ها، واپایش، خط‌مشی‌ها، استانداردها یا قوانین و مقررات (به‌عنوان ارزیابی تأثیر حفظ حریم خصوصی) تعیین می‌کنند، تنها در صورتی الزامی هستند که به‌کارگیری این واپایش‌ها سازگار با انواع اطلاعات و سامانه‌های اطلاعاتی تحت پوشش قوانین قابل‌اجرا، دستورات اجرایی، دستورالعمل‌ها، خط‌مشی‌ها، استانداردها یا مقررات باشد.

ب-۱-۷ ملاحظات مربوط به توانمندی و کارایی

واپایش‌های امنیتی با توجه به وسعت و دقت پیاده‌سازی واپایش‌ها ازنظر کارایی قیاس پذیر هستند. قدرت توانمندی و کارایی با توجه به طبقه‌بندی امنیتی سامانه اطلاعاتی به‌وسیله FIPS199 [1] مشخص می‌شود. برای مثال یک برنامه احتمالی برای سامانه اطلاعاتی با تأثیر بالا FIPS199 می‌تواند بسیار طولانی بوده و حاوی مقدار قابل‌توجهی از جزئیات پیاده‌سازی آن باشد. در مقابل برنامه احتمالی برای سامانه اطلاعاتی با تأثیر اندک FIPS199 می‌تواند به‌طور قابل‌توجهی کوتاه بوده و حاوی جزئیات پیاده‌سازی اندکی باشد. سازمان‌ها باید اختیاراتی در پذیرش واپایش‌های امنیتی سامانه‌های اطلاعاتی داشته و به قیاس پذیری عوامل در محیط‌های خاص توجه داشته باشند، این روش رویکردهای مقرون‌به‌صرفه و مبتنی بر مخاطره جهت پیاده‌سازی واپایش‌های امنیتی که منابع زیادی بیش‌ازحد لزوم صرف نمی‌کند را تسهیل می‌بخشد و درعین‌حال دست‌یابی به کاهش مخاطره، به‌اندازه کافی و مناسب فراهم می‌شود.

ب-۱-۸ ملاحظات مبتنی بر اهداف امنیتی

واپایش‌های امنیتی که به‌طور منحصربه‌فردی از موضوعات محرمانه یا اهداف امنیتی در دسترس، حمایت می‌کند؛ می‌تواند بر اساس واپایش‌های 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- به‌وسیله ارزیابی مخاطره سازمانی حمایت شود.

۳- بر اطلاعات امنیتی در سامانه اطلاعاتی اثر نگذارد.

واپایش‌های امنیتی زیر توصیه می‌شود:

۱- واپایش‌های 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- واپایش‌های بررسی صحت و درستی SC-8،

۳- واپایش‌های دسترس‌پذیری:

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

ب-۲ طبقه‌بندی واپایش‌های امنیتی

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

1 - Federal Information Processing Standard Publication 199

جدول ب-۱- طبقه‌بندی واپایش‌های امنیتی، ذکر شرح و کوته نوشت آن

شناسه	خانواده	شرح	طبقه‌بندی
AC	Access Control	واپایش 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	طرح‌ریزی احتمالی	عملیاتی
IA	Identification and Authentication	شناسایی و احراز هویت	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	طرح‌ریزی	مدیریتی
PS	Personnel Security	امنیت کارکنان	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 زیرمجموعه‌ها در طبقه‌بندی واپایش دسترسی

این بند تلاش می‌کند مواردی را تعیین کند که می‌تواند در ایجاد کاربرد واپایش‌های امنیتی مورداستفاده باشد و در ارتباط با واپایش دسترسی مطرح‌شده و مطابق با SP800-53 Rev.3 باشد.

جدول ب-۲- طبقه‌بندی واپایش امنیتی و خطوط راهنمای واپایش‌های امنیتی برای تأثیرگذاری کم، متوسط و زیاد سامانه‌های اطلاعاتی

شماره واپایش	نام واپایش			
	واپایش دسترسی	کم	متوسط	زیاد
AC-1	خط‌مشی واپایش دسترسی و روش‌ها	AC-1	AC-1	
AC-2	مدیریت حساب	AC-2	AC-2(1)(2)(3)(4)	AC-2(1)(2)(3)(4)
AC-3	اجرای دسترسی	AC-3	Ac-3(1)	AC-3(1)
AC-4	اجرای جریان اطلاعاتی	انتخاب‌نشده	AC-4	AC-4
AC-5	تفکیک وظایف	انتخاب‌نشده	AC-5	AC-5
AC-6	کمینه امتیاز	انتخاب‌نشده	AC-6	AC-6
AC-7	تلاش‌های ورود ناموفق	AC-7	AC-7	AC-7
AC-8	هشدار استفاده از سامانه	AC-8	AC-8	AC-8
AC-9	هشدار ورود قبلی	انتخاب‌نشده	انتخاب‌نشده	انتخاب‌نشده
AC-10	واپایش همزمان جلسه	انتخاب‌نشده	انتخاب‌نشده	AC-10
AC-11	موانع جلسه	انتخاب‌نشده	انتخاب‌نشده	AC-11
AC-12	اتمام جلسه	انتخاب‌نشده	AC-12	AC-12(1)
AC-13	نظارت و بررسی- واپایش دسترسی	AC-13	AC-13(1)	AC-13(1)
AC-14	عملیات مجاز، شناسایی و تأیید	AC-14	AC-14(1)	AC-14(1)
AC-15	نشان خودکار	انتخاب‌نشده	انتخاب‌نشده	AC-15
AC-16	برچسب خودکار	انتخاب‌نشده	انتخاب‌نشده	انتخاب‌نشده
AC-17	دسترسی از دور	AC-17	AC-17(1)(2)(3)(4)	AC17(1)(2)(3)(4)
AC-18	محدودیت دسترسی	AC-18	AC-18(1)	AC-18(1)(2)
AC-19	واپایش دسترسی برای افزاره‌های قابل جابجایی و انتقال	انتخاب‌نشده	AC-19	AC-19
AC-20	استفاده از سامانه‌های اطلاعاتی خارجی	AC-20	AC-19,AC-20(1)	AC-19,AC-20(1)

ب-۴ دسترسی جزئی به طبقه‌بندی واپایش

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

خانواده: واپایش دسترسی **رده**: فناوری

ب-۴-۱ AC-1 دسترسی به خط‌مشی واپایشی و فرایندها

واپایش: توسعه سازمان، انتشار و بررسی دوره‌ای/ به‌روزرسانی

۱- دسترسی رسمی و مستند به واپایش خط‌مشی 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 خط‌مشی واپایشی دسترسی و واپایش‌های دسترسی وابسته

راهنمایی بیشتر: خط‌مشی واپایش دسترسی و روش‌های سازگار با قوانین قابل‌اجرا، دستورات اجرایی، دستورالعمل‌ها، خط‌مشی‌ها، مقررات، استانداردها و راهنمایی هستند. خط‌مشی‌های واپایش دسترسی می‌تواند بخشی از خط‌مشی‌های کلی امنیت اطلاعات برای سازمان تلقی شود. فرایندهای واپایش دسترسی می‌توانند به‌طورکلی برای برنامه‌های امنیتی و همچنین برای یک سامانه اطلاعاتی به‌طور خاص، زمانی که موردنیاز است، توسعه یابند. انتشارات ویژه NIST800-12 راهنمایی در مورد خط‌مشی‌های امنیتی و فرایندها فراهم می‌کند.

اولویت و پایه تخصیص:

توسعه واپایش	Low AC-1	MOD AC-1	High AC-1

ب-۴-۲ AC-2 مدیریت حساب

واپایش: 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 مورداستفاده قرار می‌گیرند یا تغییرات دیگری رخ می‌دهد.

۹- اعطای دسترسی به سامانه اطلاعاتی بر اساس:

الف- اطلاعات معتبر که به‌وسیله وظایف رسمی اتخاذشده تعیین می‌شوند و ایجاد رضایت در مورد معیارهای امنیتی شخصی

ب- استفاده از سامانه درنظرگرفته‌شده

سایر رهنمودها:

شناسایی کاربران مجاز سامانه اطلاعاتی و تعیین دسترسی به حقوق/امتیاز مطابق با نیازهایی که در سایر واپایش‌های امنیتی در برنامه‌های امنیتی است. واپایش‌های 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 واپایش:

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 غیرفعال را از کار می‌اندازد [تخصیص: دوره زمانی تعیین‌شده‌ی 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 تعیین‌شده‌ی سازمان] جهت تأیید حساب‌های موقت و منقضی شده یا انتقال کاربرانی که مطابق باخط‌مشی‌های 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 پایین	سطح متوسط	سطح بالا
AC-2	AC-2 (1) (2) (3) (4) (5) (6)	AC-2 (1)(2)(3)(4)(5)(6)

ب-۴-۳ AC-17 دسترسی از دور

واپایش: سازمان

۱- اسناد، روش‌های دسترسی از دور به سامانه اطلاعاتی را مجاز می‌داند.
۲- ایجاد محدودیت در استفاده و راهنمای پیاده‌سازی برای هر یک از روش‌های دسترسی از دور
۳- اجازه دسترسی از دور به سامانه اطلاعاتی قبل از اتصال
۴- نیازهای موردنیاز اتصال از دور به سامانه اطلاعاتی

راهنمایی تکمیلی: دسترسی از 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 واپایش (برای مثال اینترنت) صورت می‌گیرد. مثال‌هایی از دسترسی از دور شامل خطوط تلفن، پهنای باند و بی‌سیم است. شبکه خصوصی مجازی زمانی که به‌اندازه کافی تامین‌شده، ممکن است به‌عنوان یک شبکه واپایش سازمانی تلقی شود. با توجه به ارتباط بی‌سیم، سیگنال‌ها در سازمان، تجهیزات را تحت واپایش دارند و به‌طورمعمول به‌عنوان واپایش خارج سازمانی تلقی می‌شوند. فناوری‌های بی‌سیم محدود به ماکروویو، ماهواره، بسته‌های رادیویی (UHF/VHF)[1] و بلوتوث نیستند. واپایش‌های دسترسی از دور برای سامانه‌های اطلاعاتی از طریق کارسازهای وب عمومی یا سامانه‌های خاصی که برای دسترسی عمومی طراحی‌شده‌اند، قابل‌اجرا هستند. اعمال محدودیت-های دسترسی به سامانه‌های اطلاعاتی مرتبط با ارتباطات از دور توسط واپایش AC-3 انجام می‌شود.NIST که انتشار ویژه 800-77 است، راهنمایی بر شبکه‌های مجازی خصوصی مبتنی بر IPSEC فراهم می‌کند.

1 - Ultra high frequency / very high frequency

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

بهبودهای واپایش:

۱- سازمان سازوکارهای خودکار جهت تسهیل نظارت و واپایش روش‌های دسترسی از دور به کار می‌گیرد.

۲- سازمان از رمزنگاری جهت حفاظت از محرمانه بودن و تمامیت دسترسی از دور واپایشی، استفاده می‌کند.

بهبود راهنمایی‌های تکمیلی: قدرت رمزنگاری سازوکار بر اساس FIPS199 انتخاب می‌شود که بر سطوح اطلاعات تأثیر می‌گذارد. (واپایش‌های مرتبط: SC-8، SC-9)

۳- سامانه‌های اطلاعاتی، دسترسی از دور را با مدیریت دسترسی به نقاط واپایشی تعیین می‌کنند.

۴- سازمان اجازه دسترسی از 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: واپایش مرتبط: AC-6

۵- سامانه‌های اطلاعاتی از دسترسی‌های بی‌سیم به سامانه با استفاده از احراز هویت و رمزبندی حفاظت می‌کنند.

راهنمایی تکمیلی: معمولاً برای کاربر، افزاره یا هر دو در صورت لزوم اعمال می‌شود.

۶- نظارت سازمان برای ارتباطات از دور غیرمجاز به سامانه‌های اطلاعاتی شامل دسترسی به نقاط غیرمجاز بی‌سیم. (سازمان فرکانسی را تعریف کرده و اگر یک ارتباط غیرمجاز کشف شود، عمل مناسبی انجام می‌دهد.)

راهنمایی تکمیلی: سازمان فعالانه برای ارتباطات غیرمجاز از دور بررسی می‌کند، که ازجمله شامل بررسی دسترسی به نقاط بی‌سیم 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 این‌که دسترسی به نقاط بی‌سیم غیرمجاز تنها محدود به این سامانه‌ها نیست، نیاز به بررسی دارند.

۷- سازمان، زمانی که قابلیت‌های شبکه بی‌سیم داخلی تعبیه‌شده در داخل سامانه اطلاعاتی، برای استفاده در نظر گرفته نشود، غیرفعال می‌شود.

۸- سازمان به کاربران اجازه نمی‌دهد که به‌طور مستقل، قابلیت‌های شبکه‌های بی‌سیم را پیکربندی کنند.

۹- سازمان تضمین می‌کند که کاربران از اطلاعات سازوکارهای دسترسی از دور در مورداستفاده و افشای غیرمجاز، حفاظت می‌کنند.

۱۰- سازمان واپایش‌های از دور را برای دسترسی تضمین می‌کند (فهرستی از کارکردهای 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 بی‌سیم شبکه‌ای را در داخل سامانه‌های اطلاعاتی، به‌جز برای مؤلفه‌های مشخص‌شده در حمایت از نیازهای خاص عملیاتی به‌طور صریح، غیرفعال می‌کند.

۱۲- سازمان قابلیت‌های شبکه‌ای بی‌سیم (بلوتوث) را در داخل سامانه‌های اطلاعاتی به‌جز برای مؤلفه‌های مشخص‌شده در حمایت از نیازهای خاص عملیاتی به‌طور صریح، غیرفعال می‌کند.

اولویت و پایه تخصیص:

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

ب-۵ تعریف واپایش امنیتی برنامه کاربردی از نمونه واپایشی SP800-53

این بخش به شیوه‌ای غیررسمی بیان می‌کند که چگونه واپایش AU-14 از SP800-53 می‌تواند از واپایش امنیتی برنامه کاربردی ساختار استاندارد ISO/IEC 27034 استفاده کند. ساختار کامل و دقیق داده‌های واپایش امنیتی برنامه کاربردی در استاندارد ISO/IEC 27034-5 موردبحث قرارگرفته است.

ب-۵-۱ واپایش AU-14 توصیف‌شده در SP800-53 Rev.3 به صورت زیر است:

بخش ممیزی AU-14

واپایش: سامانه اطلاعاتی قابلیت‌های زیر را فراهم می‌کند:

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

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

تکمیل بخش راهنما: فعالیت‌های جلسات ممیزی مطابق با قوانین[1] قابل‌اجرا، دستورات اجرایی، دستورالعمل‌ها، خط‌مشی‌ها و مقررات توسعه می‌یابند، یکپارچه و استفاده می‌گردند.

بهبود واپایش:

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

مرجع : ندارد

اولویت و پایه تخصیص

سطح پایین	سطح متوسط	سطح بالا
انتخاب‌نشده	انتخاب‌نشده	انتخاب‌نشده

ب-۵-۲ :بررسی واپایش AU-14 به صورت واپایش امنیتی برنامه کاربردی مطابق با استاندارد ISO/IEC 27034

1 - laws

همان‌گونه که در جدول ب-۳ در زیر توصیف‌شده است، واپایش AU-14 می‌تواند به‌عنوان چرخه توسعه امنیت در تطابق با استاندارد ISO/IEC 27034 شرح داده شود:

جدول ب-۳- واپایش SP800-53 توصیف‌شده طبق واپایش AU-14و استفاده از استاندارد ملی ISO/IEC27034

زمینه	شرح	ارزش
شناسایی ASC		
برچسب ASC-AU-14 - Id	متن: نام ASC	جلسه ممیزی
ASC-AU-14_Id-UID	متن: شماره شناسایی ASC	ASC-AU-14
توصیف-ASC-AU-14_Id	متن: توصیف ASCدر متن ساده	سامانه اطلاعاتی قابلیت‌های زیر را فراهم می‌کند: الف- ضبط و ثبت و ورود کلیه مطالب مرتبط با جلسات کاربر ب- بررسی از دور تمام مطالب مرتبط با جلسه ایجاد کاربر در زمان واقعی راهنمایی تکمیلی: فعالیت‌های ممیزی جلسات توسعه‌یافته، یکپارچه‌شده و در مشاوره با وکیل استفاده می‌شود.
نام پدیدآورنده ASC-AU-14_Id	متن: نام خانوادگی، نام،	Webu, Daming
نام شرکت پدیدآورنده ASC-AU-14_Id	متن:	شرکت ACME
رایانامه نویسنده ASC-AU-14_Id	متن: آدرس رایانامه	Wdaming@ACME.com
امضا نویسنده ASC-AU-14_Id	متن: نام ASC	894735897073420527906724 8
سازمان ASC-AU-14_Id	شناسه سازمان	JTC1/SC27 WG4 27034-1 WD3 01-001
تاریخ ایجاد ASC-AU-14_Id	تاریخ: yyyy-mm-dd	2009-04-08
اشاره به منبع ASC-AU-14_Id	منبع ASC یا بدون ارزش	بی‌ارزش
اشاره به واحد تبعی ASC-AU-14_Id	ASC واحد تبعی: فهرست شناسایی ASC یا بدون ارزش	بی‌ارزش
اشاره به زمینه کسب‌وکار ASC-AU-14_Id	فهرست B: بدون ارزش (تهی) یا دارای مفاد	مالی
اشاره به زمینه نظارتی ASC-AU-14_Id	فهرست R : بدون ارزش (تهی) یا دارای مفاد	قانون خصوصی RE76G7، ماده ۴-۱۱
اشاره به زمینه فناوری ASC-AU-14_Id	فهرست T: بدون ارزش یا دارای مفاد	بدون ارزش
مشخصات ASC-AU-14_Id	ویژگی‌های کاربردی که نیازهای امنیتی برای ASC فراهم می‌کند.	نرم‌افزار ایجاد یک جلسه مداوم
متن XML ASC-AU-14_Id	شمای ASC XML: شماره متن	v1.0 Beta

زمینه	شرح	ارزش
اهداف ASC		
سطح اعتماد- ASC-AU-14_Obj	تعداد ۱ یا n- سطح اعتماد هدف‌گذاری شده: که در این سطح اعتماد، ASC فعال بوده و ممکن است با سطوح مختلفی مرتبط باشد.	5, 6, 7, 8, 9.
دلیل- ASC-AU-14_Obj	چرا ASC وجود دارد. شناسایی نیازها برای مدیر، راهبر گروه، گروه توسعه، ممیز و ... همچنین طبق هدف، مختصراً بررسی می‌شود چه مواردی ارزیابی خواهد شد.	حصول اطمینان از این‌که کاربر مطابق با قانون حریم خصوصی #RF76G7، ماده ۴-۱۱ و استفاده از خط‌مشی‌های موردپذیرش سازمان
سطح اعتماد، دلیل--ASC-AU-14_Obj		جلسه ممیزی دارای منابع فشرده بوده و تنها موردنیاز برنامه‌های کاربردی است که اطلاعات شخصی را بامهارت انجام می‌دهد.
سطح اعتماد ، مجموع سطوح ASC-AU-14_Obj	محدوده سطوح اعتماد مورداستفاده سازمان	واپایش‌های ۰،۱،۲،۳،۴،۵،۶،۷،۸،۹
ASC-AU-14 -App Spec. - ComplToReg - Stds&BestPractices	استانداردهایی که همراه با ASC هستند.(Cobit، ITIL، RUP، استـانـدارد ISO 17799، design pattern name، etc)	NIST SP-800-53 Rev. 3, AU-14
فعالیت امنیتی ASC		
ASC-AU-14_secAct-برچسب	متن: نام فعالیت	پیاده‌سازی جلسه ممیزی، با توجه به سطح امنیتی تأییدشده 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 کتابخانه امنیتی JAVA که توسط سازمان تاییدشده است برای پیاده سازی فرایند جلسات ممیزی امن در برنامه کاربردی استفاده نمایید.
ASC-AU-14_secAct پیچیدگی	سطح پیچیدگی فعالیت: ساده، استاندارد، پیچیده، بسیار پیچیده	ساده
ASC-AU-14_secAct نقش افراد	نقش موجود در سازمان	توسعه‌دهنده
ASC-AU-14_secAct مسئولیت فرد	تحقق و مشارکت	تحقق و پیاده‌سازی

زمینه	شرح	ارزش
ASC-AU-14_secAct صلاحیت فرد	احراز صلاحیت فرد: ارائه‌کننده شرایط موردنیاز افراد	سطح توسعه‌دهندگی متوسط یا بیشتر
ASC-AU-14_secAct زمان	مورد هدف قرار دادن یک فعالیت در استاندارد ISO/IEC27034، کاربرد امنیتی مدل مرجع چرخه حیات	مرحله توسعه، واحد توسعه فعالیت
ASC-AU-14_secAct فراورده	فراورده: نام شرح فراورده تولیدشده توسط این فعالیت	بررسی مورد مرتبط JAVA
ASC-AU-14_secAct نتایج- انتظارات	نتایج مورد انتظار، موقعیت، وضع یا ارزش دقیق فراورده	برای هر معامله، نیاز به ارسال معاملات ویژه به بخش خدماتی و امنیتی سازمان است. نتایج آزمون این واحد و مدارک آن در پایان این فعالیت مورد انتظار است.
ASC-AU-14_secAct هزینه	هزینه فعالیت: هزینه‌ای برای اتمام این فعالیت در نظر گرفته می‌شود.(پول- روز/فرد و ...	۱۰ نفر-روز
تأیید سنجش ASC		
ASC-AU-14_VerfMeas برچسب		تأیید اجرا و پیاده‌سازی مؤلفه‌های جلسات ممیزی
ASC-AU-14_VerfMeas-UID:		.VeM-001-JAVA453
ASC-AU-14_VerfMeas- توضیحات		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 می‌شود.
ASC-AU-14_VerfMeas- پیچیدگی	تأیید پیچیدگی‌های اندازه‌گیری: ساده، استاندارد، پیچیده، بسیار پیچیده	استاندارد
ASC-AU-14_VerfMeas- نقش فردی	نتایج مورد انتظار، موقعیت، وضع یا ارزش دقیق فراورده	بازبینی کد
ASC-AU-14_VerfMeas- مسئولیت	تحقق - مشارکت	تحقق
ASC-AU-14_VerfMeas- صلاحیت فردی	صلاحیت واپایش فعالیت: ارائه مدارک موردنیاز افراد	توسعه‌دهنده JAVA
ASC-AU-14_VerfMeas- زمان - مراحل	فعالیت مورد هدف در کاربرد امنیتی مدل مرجع چرخه حیات	مرحله توسعه، فعالیت آزمون کارکرد
ASC-AU-14_VerfMeas- محصول فرعی		نتایج باید برای تمام تأییدهای سنجش صحیح باشد
ASC-AU-14_VerfMeas-	بهای تمام‌شده فعالیت واپایشی: هزینه	۱ نفر-روز

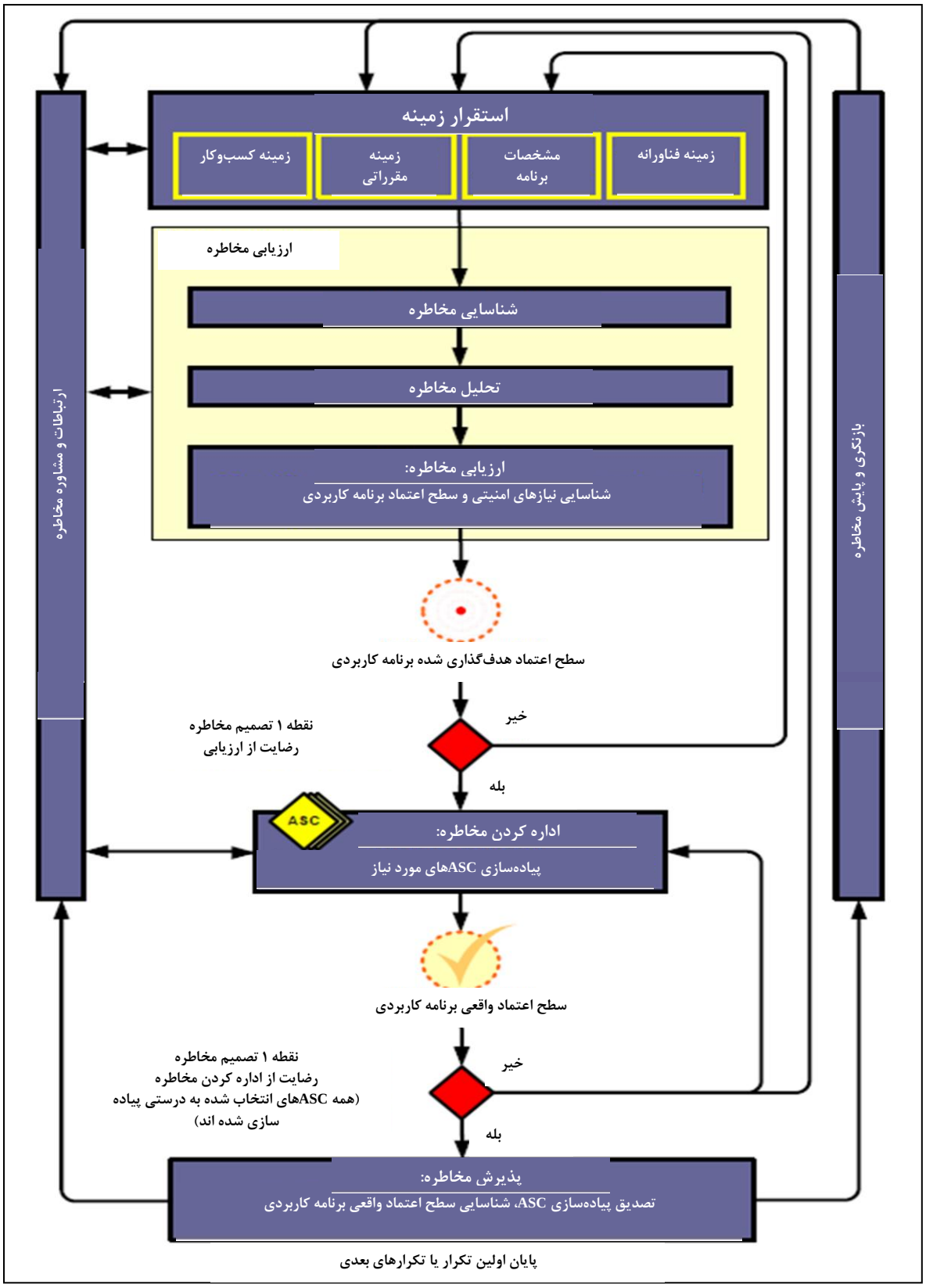
زمینه	شرح	ارزش
بهای تمام‌شده	برای تأیید این فعالیت(فرد/روز، پول و ...) واضح است که ارزیابی دوره‌ای الزامی خواهد بود.	

پیوست پ

(اطلاعاتی)

فرایند مدیریت مخاطره در استاندارد ملی ایران به شماره : ۲۷۰۰۵ نگاشت شده با فرایند مدیریت امنیت برنامه کاربردی(ASMP)

فرایند کاربردی مدیریت امنیت را از نقطه‌نظر مخاطره در نظر می‌گیریم. بنابراین یک فرایند مشابه فرایند مدیریت مخاطره طبق استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲ تعریف می‌شود.



شکل پ-۱- فرایند مدیریت مخاطره در استاندارد ملی ایران به شماره ۲۷۰۰۵ نگاشت شده با فرایند مدیریت امنیت برنامه کاربردی

عناصر فرایندی که در ادامه می‌آید انجام می‌شوند. در ابتدا زمینه برنامه کاربردی تعیین‌شده است؛ سپس ارزیابی مخاطره در سطح برنامه کاربردی انجام‌شده است. اگر این موارد اطلاعات کافی برای تعیین واپایش‌هایی که برای کاهش مخاطرات به درجه‌ای قابل‌قبول (یا قابل‌تحمل) برای مالک برنامه کاربردی جهت استفاده سازمان از برنامه کاربردی فراهم کند، سپس این وظیفه تکمیل و راه‌های رفع این مخاطره دنبال می‌شود. اگر اطلاعات ناکافی باشد، ارزیابی مخاطره مجدداً با معیارهای تجدیدنظر شده مخاطره و محیط‌های کاربردی (برای مثال، زمینه کسب‌وکار، زمینه نظارتی و فناورانه، 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 نیازهای امنیتی نشأت‌گرفته برای یک برنامه کاربردی به‌خوبی مشخص نشود، برنامه کاربردی به‌اندازه کافی امن نخواهد بود؛ زیرا نیازهای امنیتی نیاز به شناسایی سطح هدف و میزان اطمینان برنامه کاربردی دارد.

امکان‌پذیر است که رفع مخاطره به‌سرعت منجر به یک سطح مخاطره موردپذیرش یا قابل‌تحمل نشود که در آن مورد، تکرار مجدد ارزیابی مخاطره با پارامترهای دقیق‌تر انجام می‌شود.(برای مثال مشخصات برنامه‌های کاربردی، نیازهای امنیتی، سطح اعتماد و واپایش برنامه‌های کاربردی موردنیاز و ...) اگر لازم باشد، امنیتی موردپذیرش توسط یک اعتبار رسمی داخلی یا خارجی موردنیاز است.

بر اساس استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲، 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. توصیه می‌شود 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 مخاطرات، سطح اعتماد و ASC های مرتبط با گروه‌های مناسبی در ارتباط 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 واپایش در مکان جهت حذف مخاطره و مکان‌های نامطمئن در سازمان منجر به‌مواجهه مناسب در رویدادهای غیرمنتظره با توجه به بهترین حالت می‌شود. همان‌گونه که در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲ تعریف‌شده، توصیه می‌شود نتایج جزئی در هر بخش از فرایند مدیریت مخاطره و از دونقطه تصمیم‌گیری مخاطره 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*