INSO-ISO-IEC
27034-2
1st.Edition
2017

Identical with
ISO/IEC
27034-2:2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
ایزو- آی ایی سی
۲۷۰۳۴-۲
چاپ اول
۱۳۹۶

دارای محتوای رنگی

فناوری اطلاعات–
فنون امنیتی–امنیت برنامه کاربردی-
قسمت ۲: چارچوب الزامی سازمان

Information technology
— Security techniques —
Application security—
Part 2:
Organization normative framework

ICS: 35.030

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri .gov.ir

به‌نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف درکمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی 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 غیر دولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح، بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که براساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1] کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه شناسی 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 پیش‌بینی شده 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 کند. سازمان می‌تواند به‌منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمانها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان استاندارد ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را براساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و درصورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، 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 Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات – فنون امنیتی– امنیت برنامه کاربردی- قسمت ۲: چارچوب الزامی سازمان»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات- سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون مدیر کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
عباسپور، مقصود (دکتری مهندسی کامپیوتر- معماری)	دانشیار– معاون مرکز فناوری دانشگاه شهید بهشتی
طباطبایی ملاذی، هادی (دکتری مهندسی کامپیوتر)	استادیار- دانشگاه شهید بهشتی
مطلق، کامبیز (کارشناسی ارشد فناوری اطلاعات)	معاون فناوری اطلاعات– بانک قوامین
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران

اعضاء : (اسامی به ترتیب حروف الفبا)

	سمت و/ یا محل اشتغال:
ناظمی، اسلام (دکتری مهندسی کامپیوتر)	دانشیار- دانشگاه شهید بهشتی
نصیری آسایش، حمیدرضا (کارشناسی ارشد فناوری اطلاعات- معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات- معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی

ویراستار:	**سمت و/ یا محل اشتغال:**
رضایی، رامین (کارشناسی مهندسی الکترونیک)	معاون طرح و توسعه - مرکز تحقیقات صنایع انفورماتیک

فهرست مندرجات

پیش‌گفتار

استاندارد « فناوری اطلاعات– فنون امنیتی– امنیت برنامه کاربردی- قسمت ۲: چارچوب الزامی سازمان» که پیش‌نویس آن در کمیسیون‌های مربـوط بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شماره ۵ تهیه و تدوین شده، در چهارصد و نود و نهمین اجلاسیه کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۶/۰۲/۱۹ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی برمبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است.

ISO/IEC 27034-2: 2015, Information technology — Security techniques — Application security— Part 2: Organization normative framework

مقدمه

کلیات

سازمان‌ها برای باقی ماندن در کسب‌وکار باید از اطلاعات و زیرساخت‌های فناورانه خود محافظت کنند. نیاز فزاینده‌ای در سازمان‌ها برای تمرکز روی حفاظت از اطلاعات خود در سطح برنامه کاربردی وجود دارد. رویکرد سامان‌مند برای بهبود امنیت برنامه کاربردی، برای سازمان به همراه شواهد، نشان می‌دهد که اطلاعات مورد استفاده قرار گرفته یا ذخیره شده توسط برنامه‌های کاربردی آن‌ها، به اندازه کافی محافظت می‌شوند.

استاندارد ISO/IEC 27034 فراهم کنندهٔ مفاهیم، اصول، چارچوب‌ها، مولفه‌ها و فرایندها برای کمک به سازمان در یکپارچه‌سازی امنیت در سراسر چرخه عمر برنامه‌های کاربردی است.

چارچوب الزامی سازمان (ONF) مهم‌ترین آن دسته از مولفه‌ها است.

چارچوب الزامی سازمان چارچوبی در گستره سازمان است که همه نمونه‌های موفق امنیت برنامه‌های کاربردی شناخته شده توسط سازمان ، در آن ذخیره می‌شود. این چارچوب از مولفه‌ها و فرایندهای ضروری تشکیل شده است که برای مدیریت خود چارچوب ONF، از این مولفه‌ها و فرایندها بهره می‌برد. این چارچوب پایه امنیت برنامه کاربردی در سازمان است و توصیه می‌شود تمام تصمیم‌گیری‌های آتی امنیت برنامه کاربردی در سازمان با ارجاع به این چارچوب انجام شود. چارچوب ONF منبعی معتبر برای تمام مولفه‌ها و فرایندهای مرتبط با امنیت برنامه کاربردی در سازمان است.

این استاندارد فرایندهای مورد نیاز برای مدیریت امنیت برنامه‌های کاربردی در سازمان را تعیین می‌کند. این فرایندها در زیربند ۵-۴ ارائه شده است. همچنین این استاندارد به معرفی عناصر مرتبط با امنیت برنامه‌های کاربردی (فرایندها، نقش‌ها و مولفه‌ها) می‌پردازد که توصیه می‌شود با ONF یکپارچه شوند. این عناصر در زیربند ۵-۵ ارائه شده است.

در پایان، این استاندارد ممیزیِ فرایند ONF را ارائه می‌کند که سازمان برای درستی‌سنجی ONF خود و درستی‌سنجی انطباق تمامی برنامه‌های کاربردی برنامه‌های با الزامات و واپایش‌ها[1] درONF به این فرایند نیاز دارد. این فرایند در زیربند ۵-۴-۸ ارائه می‌شود.

مقصود[2]

مقصود این استاندارد کمک به سازمان برای ایجاد، نگه‌داری و اعتبارسنجیِ چارچوبONF خود در انطباق با الزامات این استاندارد است.

1 - Control
2 - Purpose

این استاندارد برای توانمند ساختن سازمان طراحی شده است تا چارچوب ONF خود را با معماریِ سازمانی و/یا الزامات سامانه مدیریت امنیت اطلاعات سازمان همسو و یکپارچه کند. با این وجود، پیاده‌سازی سامانه مدیریت امنیت اطلاعات به‌گونه‌ای که در استاندارد ISO/IEC 27001 شرح داده شده است، برای پیاده‌سازی این استاندارد، الزامی نیست.

مخاطبان هدف

مخاطبان در هنگام انجام نقش‌های تعیین‌شده سازمانی خود، به ارزش و منفعت خواهند رسید:

الف- مدیران

ب- کارگروه ONF

پ- کارشناسان حوزه[1]

ت- ممیزان[2]

مدیران

توصیه می‌شود مدیران این استاندارد را مطالعه کنند، چون در موارد مسئولیت دارند:

الف- بهبود امنیت برنامه کاربردی از طریق ONF و دیگر جنبه‌های استاندارد ISO/IEC 27034؛

ب- حصول اطمینان از این‌که ONF با سامانه مدیریت امنیت اطلاعات و نیازهای امنیت برنامه کاربردی سازمان همسو باشد؛

پ- رهبریِ ایجاد[3] ONF در سازمان؛

ت- حصول اطمینان از این‌که ONF در دسترس بوده و ابلاغ شده باشد و در پروژه‌های برنامه‌کاربردی به همراه ابزارها و رویه‌های مناسب در سراسر سازمان استفاده می‌شود؛

ت- تعیین سطح (سطوح) مقتضی مدیریت که کارگروه ONF به آن گزارش می‌دهد.

کارگروه[4] ONF

کارگروه ONF مسئول مدیریت پیاده‌سازی و نگه‌داری مولفه‌ها و فرایندهای مرتبط با امنیت برنامه کاربردی در چارچوب الزامی سازمان است. نیاز است کارگروه ONF:

الف- هزینه پیاده‌سازی و نگه‌داری ONF را مدیریت کند؛

ب- تعیین کند که چه مولفه‌ها و فرایندهایی بهتر است در ONF پیاده‌سازی شود؛

1 - Domain experts
2 - Auditors
3 - Establishment
4 - Committee

پ- اطمینان داشته باشد که مولفه‌ها و فرایندهای معرفی شده، اولویت‌های سازمان برای الزمات امنیت را رعایت می‌کند؛

ت- بازنگریِ گزارش‌های ممیز برای پذیرش یا رد این‌که ONF با استاندارد انطباق دارد و الزامات سازمان را برآورده می‌کند؛

ث- فرایندها و ابزارهای مدیریت انطباق با استانداردها، قوانین و مقررات مطابق با مقررات سازمان را فراهم کند؛

ج- آگاهی‌های امنیتی، آموزشی و نظارتی به تمامی کنش‌گران ابلاغ کند و

چ- ارتقای انطباق با ONF برای تمامی پروژه‌های برنامه‌کاربردی در سراسر سازمان.

گروه توسعه ONF

کارشناسانی که از طریق کارگروه ONF منتسب شده‌اند تا کار توسعه و پیاده‌سازی یک یا چند عنصر ONF را انجام دهند، نیاز است تا:

الف- عنصر طراحی شده ONF را توسعه داده و پیاده‌سازی کنند،

ب- آموزش استفاده از عناصر ONF، به‌وسیله کنش‌گران مختلف خود را تعیین کنند و

پ- در ارائه آموزش کافی به کنش‌گران همکاری کنند.

کارشناسان حوزه

کارشناسان تدارک، عملیات، اکتساب و ممیزی که نیاز است:

الف- در پیاده‌سازی و نگه‌داری ONF شرکت داشته باشند،

ب- اعتبارسنجی کنند که ONF در پروژه برنامه‌کاربردی قابل استفاده و سودمند است و

پ- مولفه‌ها و فرایندهای جدید را پیشنهاد دهند.

ممیزان

ممیزان کارکنانی هستند که نقش‌هایی را در فرایندهای ممیزی انجام می‌دهند و ممیزان کسانی هستند که نیاز است در اعتبارسنجی و درستی‌سنجی ONF شرکت داشته باشند.

یادآوری- ممکن است بسته به هدف و شرایط ممیزی و با توجه به خط‌مشی‌های ممیزی و الزامات انطباق سازمان، ممیزان به داخل یا بیرون سازمان تعلق داشته باشند.

فناوری اطلاعات– فنون امنیتی– امنیت برنامه کاربردی- قسمت ۲: چارچوب الزامی سازمان

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و ارائه توصیف مفصلی از چارچوب الزامی سازمان و ارائه راهنمای پیاده‌سازی این چارچوب برای آن سازمان‌ها است.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آنها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

۲-۱ فناوری اطلاعات– فنون امنیتی - امنیت برنامه کاربردی قسمت ۱: مرور کلی و مفاهیم

یادآوری- جزییات بیشتر در مورد ارتباط بین استاندارد ISO/IEC 27034 و دیگر استانداردها در بند ۰/۵ از استاندارد ISO/IEC 27034-1:2011 در دسترس است.

2-2 ISO/IEC 27000, Information technology — Security Techniques — Information security management systems — Overview and vocabulary

2-3 ISO/IEC 27005, Information technology — Security techniques — Information security risk management

یادآوری- استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات، با استفاده از استاندارد ISO/IEC 27005: 2011 تدوین شده است.

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف مطرح شده در استانداردهای ISO/IEC 27034-1، ISO/IEC27000 و ISO/IEC27005 به‌کار می‌روند.

۴ کوته‌نوشت‌ها

چرخه عمر امنیت برنامه کاربردی	ASLC Application Security Life Cycle
مدل مرجع برای چرخه عمر امنیت برنامه کاربردی	ASLCRM Application Security Life Cycle Reference Model
چارچوب الزامی برنامه کاربردی	ANF Application Normative Framework
واپایش امنیت برنامه کاربردی	ASC Application Security Control
فرایند مدیریت امنیت برنامه کاربردی	ASMP Application Security Management Process
چارچوب الزامی سازمان	ONF Organization Normative Framework

۵ چارچوب الزامی سازمان

۵-۱ کلیات

چارچوب الزامی هر سازمان مجموعه‌ای است از همهٔ مقررات، خط‌مشی‌ها، روش‌ها، نقش‌ها و ابزارهایی است که آن سازمان به کار می‌گیرد. بهتر است هر سازمان از پیش چارچوب الزامی- کمابیش برخوردار از مستندسازی رسمی- داشته باشد.

مفهوم چارچوب الزامی سازمان که در این استاندارد توصیف می‌شود، یک چارچوب وسیع سازمانی گسترده-ای است، دربردارندهٔ: زیرمجموعه‌ای از فرایندها و مولفه‌های سازمان در ارتباط با امنیت برنامه کاربردی است که از الزام درون-سازمانی برخوردارند.

اگرچند که گام نخست در امن‌سازی برنامه‌های کاربردی سازمان، برخورداری از ONF غیررسمی است؛ این استاندارد، به کارگیری ONF رسمی و استاندارد شده ای را- آنگونه که در همین استاندارد توصیف شده است- توصیه می‌کند.

۵-۲ مقصود

مقصود از پیاده‌سازی ONF این است که:

الف- برای امنیت برنامه کاربردی مسئولیت اختصاص یابد و فرایندی ایجاد شود که قابلیت تغییر برای بهبود قابلیت مشاهدهٔ امنیت برنامه کاربردی را دارد.

ب- اطمینان از اینکه همه عناصر (مولفه‌ها، نقش‌ها و فرایندها) در ارتباط با امنیت برنامه کاربردی توسط افراد تصمیم گیرنده ذی‌صلاح تایید شده و توسط بازیگران و ذی‌نفعان پذیرفته می‌شود.

پ- کمینه کردن مقاومت در برابر تغییرات ایجاد شده توسط عناصر جدید امنیت برنامه کاربردی

ت- استانداردسازی عناصر امنیت برنامه کاربردی برای اطمینان از پیاده‌سازی یکنواخت و تایید آن در سراسر سازمان.

ث- کمک به بهبود سطح بلوغ سازمان (طبق تعریف مطرح شده در استاندارد ISO/IEC 15504 و دیگر استانداردها مانند SEI/CMMI) توسط رسمی‌سازی و ممیزی همه کاربردهای عناصر امنیت برای به‌روز نگهداشتن آن‌ها با محیط تغییر سازمان و

ج- ایجاد سازوکارهایی برای تضمین اینکه سطح مناسبی از امنیت می‌تواند در حالت موثری به‌عنوان مثال از طریق استفاده مجدد عناصر امنیت برنامه کاربردی تایید شده موجود، به‌دست آید.

۵-۳ اصول

توصیه می‌شود سازمان‌ها برای ایجاد و حفظ مولفه‌ها و فرایندها در ONF طبق اصول زیر هدایت شوند:

الف- توصیه می‌شود محتویات ONF سازگار با نیازهای کسب و کار سازمان شود.

ب- توصیه می‌شود هر عنصر تعریف شده‌ای در ONF توسط کارگروه ONF تایید شود.

پ- توصیه می‌شود محتویات ONF قابل دسترس بوده و در سطح وسیع سازمان بتوان آن را ابلاغ کرد.

ت- به علت اینکه زمینه تهدید به‌طور مداوم و بی‌خبر تغییر می‌کند، توصیه می‌شود سازمان برای بازنگری ONF، در پاسخ به این تغییرات آماده شود.

ث- توصیه می‌شود ONF قابل ممیزی باشد.

۵-۴ فرایند مدیریت ONF

۵-۴-۱ کلیات

توصیه می‌شود سازمان، فرایندی در سطح سازمان برای مدیریت ONF خود ایجاد، پیاده‌سازی، نگهداری کند و آن را بهبود بخشد.

فرایند مدیریت ONF از شش فرایند فرعی تشکیل می‌شود.

چهار مورد از این فرایندهای فرعی با فرایندهای طرح، انجام، بررسی، اقدام، مربوط به مدل عمومیPDCA[1] هستند و متناسب با توسعه و پیاده‌سازی عناصر امنیت برنامه کاربردی در ONF در نظر گرفته می‌شوند.

جدول ۱ نشان می‌دهد که چگونه مدیریت ONF با چهار مرحله مدل PDCA و فرایندهای سامانه مدیریت امنیت مطابقت می‌یابد.

1-Plan, Do, Check, Act

جدول ۱- نگاشت مراحل PDCA، فرایندهای سامانه مدیریت امنیت اطلاعات و زیرفرایندهای مدیریت ONF مرتبط با امنیت برنامه کاربردی

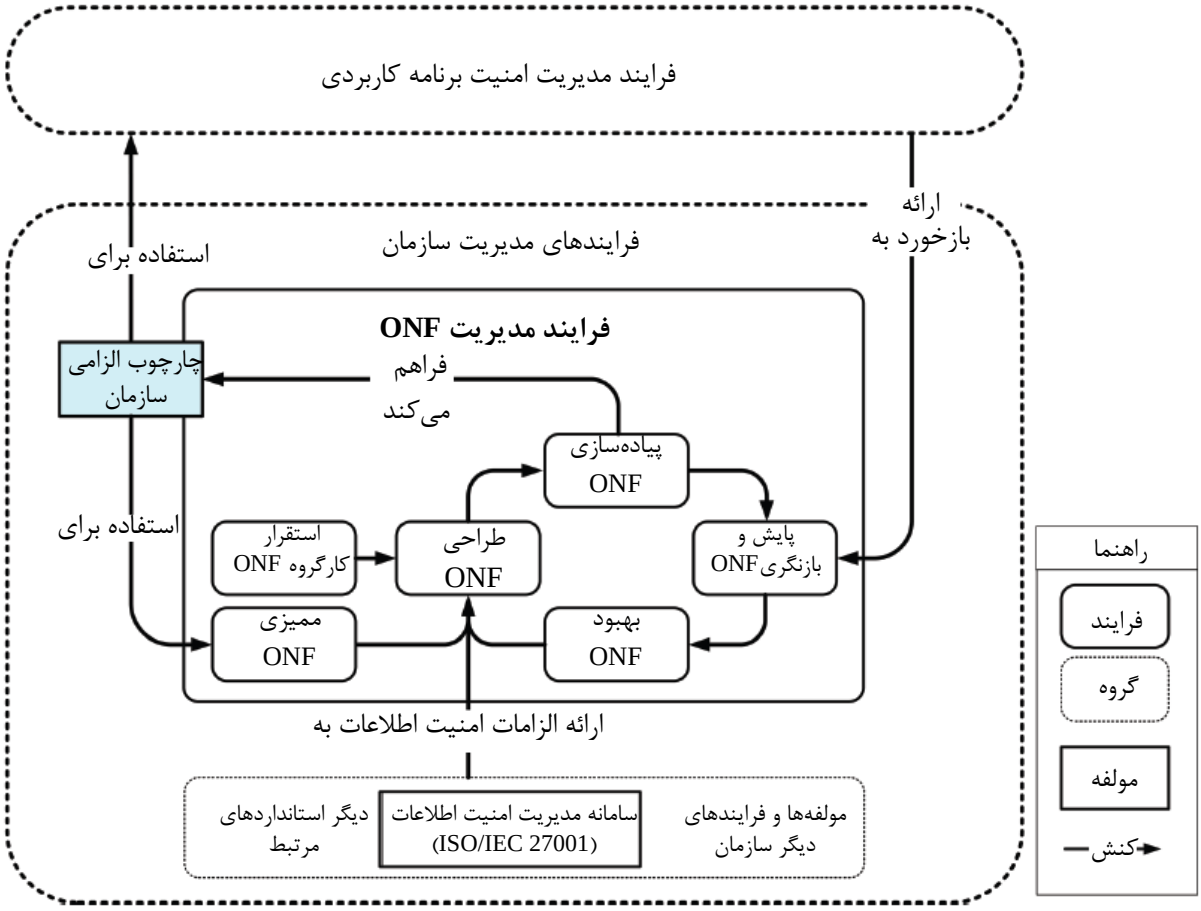
مرحله PDCA	ISO/IEC 27001 فرایند مدیریت امنیت اطلاعات	ISO/IEC 27034 فرایند مدیریت ONF
طرح	طرح‌ریزی	طراحی ONF
انجام	حمایت/ عملیات	پیاده‌سازی ONF
بازبینی	ارزشیابی کارایی	پایش و بازنگری ONF
اقدام	بهبود	بهبود ONF

زیرفرایند دیگر، یعنی ایجاد کارگروه ONF در آغاز برای ملزم کردن کارگروه ONF به نمایش تعهد مدیریت مناسب در قبال امنیت برنامه کاربردی به کار می‌رود و سرانجام، زیرفرایند ممیزی ONF برای درستی‌سنجی ONF و انطباق کاربردها با الزامات و واپایش‌ها در ONF به‌کار برده می‌شود.

به سازمان توصیه می‌شود که فرایند مدیریت ONF را به‌طور تکراری برای پیاده‌سازی افزایشی ONF انجام دهد. این اقدام، تأثیر را کاهش داده و از طریق اولویت‌بندی در هر تکرار، عناصری که نیازهای با اولویت بالاتری دارند، سریع‌تر به دستاوردهای مربوط دست می‌یابند.

نمود نگاشتاری[1] فرایند مدیریت ONF را در شکل ۱ نشان داده شده است. شکل مذکور نیز نحوه ارتباط این فرایند با دیگر فرایندهای مدیریت سازمان و فرایند مدیریت امنیتی را نشان می‌دهد که کاربرد ONF را برای افزودن واپایش‌های امنیت برنامه کاربردی به پروژه‌های برنامه کاربردی امکان‌پذیر می‌کند.

1 - Graphical



شکل-۱ فرایند مدیریت ONF

۲-۴-۵ استفاده از نمودارهای RACI[1] در توصیف فعالیت‌ها، نقش‌ها و مسئولیت‌ها

این استاندارد از نمودارهای RACI برای انتساب نقش‌ها و مسئولیت‌ها در انجام فعالیت‌ها در فرایندها استفاده می‌کند. چنین نمودارهایی مسئولیت و پاسخ‌گویی بازیگران را در مشاوره یا آگاهی برای تحقق[2] فعالیت مشخص می‌کند. کوته‌نوشت‌ها برای توصیف مسئولیت‌های بازیگران استفاده می‌شوند. این کوته-نوشت‌ها در جدول ۲ برشمرده می‌شوند.

جدول ۲- کوته‌نوشت‌های مورد استفاده در نمودارهای RACI مربوط به مسئولیت‌های بازیگران

کد	مسئولیت
R	مسئول تحقق فعالیت
A	پاسخگو در قبال تحقق فعالیت
C	مورد مشورت در طول تحقق فعالیت
I	آگاهی از تحقق فعالیت

1 - Responsible, Accountable, Consulted, Informed
2 - Realization

برای استفاده از نمودارهای RACI در سازمان‌ها، نیازی به پیاده‌سازی این استاندارد وجود ندارد. به سازمان‌ها توصیه می‌شود که راهنمای ارائه شده در این استاندارد را با روش وضوح نقش‌ها و مسئولیت‌ها همسو کنند.
هنگام اجرای فعالیت‌های تحقق و درستی‌سنجی، تعیین منابعی که مسئول، پاسخگو، مشاور و آگاه هستند، برای سازمان امری حساس تلقی می‌شود. جداول زیر نقطه شروعی را برای بحث طی تحقق ONF فراهم می‌آورد.

۵-۴-۳ تأسیس کارگروه ONF

۵-۴-۳-۱ مقصود

مقصود از این فرایند، تأسیس کارگروه ONF با اختیار و منابع مورد نیاز برای توسعه، پیاده‌سازی و تغییر ONF و به نمایش نهادن تعهد مدیریت مناسب پاسخگو است.

۵-۴-۳-۲ نتایج

نتیجه عملکرد موفق این فرایند به شرح زیر است:

الف- نقش‌ها و مسئولیت‌ها برای اعضای کارگروه ONF تعریف می‌شوند.

ب- داوطلبی به هر نقش منتسب می‌شود.

پ- کارگروه ONF به لحاظ رسمی ملزم به تأسیس و حفظ چارچوب ONF می‌شوند و این موضوع در داخل سازمان ابلاغ می‌شود.

ت- کارگروه ONF پاسخگوی پیاده‌سازی، کیفیت و کاربرد چارچوب ONF در سازمان می‌شود.

ث- منابع لازم با توجه به مسئولیت‌های کارگروه ONF فراهم می‌شود و

ج- به کارگروه ONF، برای ارتباط داخلی مرتبط، اختیار کافی داده می‌شود.

۵-۴-۳-۳ فعالیت‌های تحقق

جدول ۳- نمودار RACI برای تحقق فرایند «تأسیس کارگروه ONF»

فعالیت‌های تحقق	مدیران
۱- تعریف نقش‌ها و مسئولیت‌ها برای اعضای کارگروه ONF	A/R
۲- انتصاب داوطلب برای هر نقش	A/R
۳- به لحاظ رسمی کارگروه ONF را ملزم به ایجاد و نگهداری ONF کرده و آن را در حیطه سازمان ابلاغ می‌کند.	A/R
۴- کارگروه ONF را پاسخگوی پیاده‌سازی ONF، کیفیت و به‌کارگیری در سازمان قرار می‌دهد.	A/R
۵- کارگروه ONF منابع ضروری را با فرض مسئولیت‌ها فراهم می‌آورد.	A/R
۶- کارگروه ONF با اختیار کافی را برای ارتباط داخلی مربوط فراهم می‌آورد.	A/R

۵-۴-۳-۴ فعالیت‌های درستی‌سنجی

جدول ۴- نمودار RACI برای درستی‌سنجی فرایند «تأسیس کارگروه ONF»

فعالیت‌های درستی‌سنجی	مدیران	ممیزین
۱- تایید وجود ارتباط رسمی از ناحیه مدیریت مناسب پاسخگو، مبنی بر دستیابی به نتایج الف، ب، پ و ت	A	R
۲- ارزشیابی ارتباط رسمی از ناحیه مدیریت مناسب پاسخگو که آیا نتایج (ث) و (ج) حاصل شدند.	A	R

۵-۴-۴ طراحی ONF

۵-۴-۴-۱ مقصود

مقصود از این فرایند، تعیین اهداف برای امنیت برنامه کاربردی، تعیین عناصر قابل توصیه برای پیاده‌سازی ONF در تکرار کنونی فرایند مدیریت ONF و طراحی عناصر مذکور است.

۵-۴-۴-۲ نتایج

نتیجه عملکرد موفقیت‌آمیز این فرایند عبارت است از:

الف- حوزه تکرار کنونی فرایند مدیریت ONF تعریف می‌شود و توسط مدیریت پاسخگوی مناسب تایید شده و ابلاغ می‌شود و

ب- عناصر داخل حوزه ONF طراحی می‌شوند.

۵-۴-۴-۳ فعالیت‌های مرتبط با تحقق‌یابی

جدول ۵- نمودار RACI برای فرایند «طراحی ONF»

فعالیت‌های تحقق	مدیران	کارگروه ONF
۱- تعیین اهداف امنیت برنامه کاربردی	A	R
۲- تعریف حوزه و دامنه پیاده‌سازی خط‌مشی تکرار جاری فرایند مدیریت ONF	A	R
۳- تعریف وضعیت، اولویت‌ها و طرح‌های امنیت برنامه کاربردی سازمان		A/R
۴- ایجاد مخزن و طبقه‌بندی امنیتی اطلاعات در ارتباط با برنامه‌های کاربردی و یکپارچگی آن با معماری اطلاعات سازمان		A/R
۵- طراحی عناصر ONF		A/R

۵-۴-۴-۴ فعالیت‌های درستی‌سنجی

جدول ۶- نمودار RACI برای درستی‌سنجی فرایند «طراحی ONF»

فعالیت‌های درستی‌سنجی	مدیران	ممیزین
۱- درستی‌سنجی اینکه دامنه کاربرد تکرار جاری فرایند مدیریت ONF تعریف شده، توسط مدیریت مناسب پاسخگو تایید و ابلاغ می‌شود.	A	R
۲- درستی‌سنجی اینکه عناصر ONF به درستی در دامنه تکرار جاری طراحی شده‌اند.	A	R

۵-۴-۴-۵ راهنمایی

ورودی‌های ممکن برای این فرایند عبارتند از:

الف- نتایج فرایند مدیریت مخاطره امنیتی مانند اهداف یا طرح‌های امنیتی در سطح سازمان.

ب- نتایج «بهبود فرایند ONF» مانند مستندسازی که به طراحی مجدد مولفه‌های ONF یا طراحی تازه مولفه‌های ONF نیاز دارد.

پ - نتایج ممیزی فرایند ONF.

ت - نتایج ممیزی امنیت اطلاعات سازمان.

ث- نیازهای آموزش، راهبرد، معیارها، خط‌مشی‌ها و به روز نگه داشتن دانش حملات و کاهش آن‌ها و

ج- دیگر استانداردهای ISO/IEC شامل زنجیره تامین (۲۷۰۳۶)، ارزشیابی (۱۵۴۰۸)، تضمین (۱۵۰۲۶)، فرایندهای چرخه عمر نرم‌افزاری (۱۲۲۰۷)، فرایندهای چرخه عمر سامانه (۱۵۲۸۸)، به استاندارد ISIRI 27034-1 و شکل ۱ مراجعه کنید.

عناصر ONF که برای طراحی توصیه می‌شود در زیربند ۵-۵ توصیف می‌شوند. راهنمای خاص برای طراحی این‌گونه اجزا نیز در زیربند ۵-۵ یافت می‌شود.

توصیه می‌شود عناصر ONF در فرایند تکراری طراحی و ساخته شود. در حین این فرایند، توصیه می‌شود کارگروه ONF:

الف- عناصر را بر مبنای اولویت‌های سازمان و منابع قابل دسترس اولویت‌بندی کند.

ب- مسئولیت و منابع کافی را برای طراحی عناصر داخل حوزه تخصیص دهد.

پ- طراحی عناصر ONF را پایش و اعتبارسنجی کند.

ت- فرایندهای ONF را در فرایندهای کسب‌وکار سازمان ادغام کند.

ث- تضمین کند که خط‌مشی امنیت برنامه کاربردی همسو با دیگر خط‌مشی‌های سازمان و سامانه مدیریت امنیتی اطلاعات است.

ج- تضمین کند که ONF با معماری امنیت سازمان، معماری اطلاعات و معماری کسب‌وکار همسو است.

چ- تضمین کند که شاخص‌های عملکرد مدیریت مخاطره ONF با دیگر شاخص‌های عملکردی مورد استفاده در سازمان همسو است.

ح- تضمین کند که اهداف مدیریت مخاطره ONF با اهداف و راهبردی‌های سازمان همسو است.

خ- تضمین الزامات مقرراتی و قانونی را تضمین کند.

د- تضمین کند که نتایج فعالیت‌ها به همه طرفین مربوط ابلاغ می‌شود.

ذ- مخزن اطلاعاتی را طراحی کند که به‌عنوان منبع معتبر برای ترکیب و ارتباط اطلاعات در مورد ONF و همه عناصر آن عمل کند.

ر- سازوکارهای ارتباطی و گزارش‌گیری (داخلی، بیرونی، واسطه‌هایی با پروژه‌های کاربردی و غیره) را ایجاد کند و

ز- از طریق ایجاد خط‌مشی مدیریت امنیت برنامه کاربردی، راهنمایی را در مورد نحوه پیاده‌سازی الزامات این استاندارد در سازمان ارائه کند.

یادآوری- نمی‌توان انتظار داشت که هر عضو یا همکار سازمان این استاندارد را بخواند. بلکه می‌توان از آن‌ها انتظار داشت که با خط‌مشی مربوط انطباق یابند.

هنگام تایید هدف و دامنه کاربرد تکرار فرایند مدیریت ONF، مدیریت مناسب پاسخگویی به شرح زیر توصیه می‌شود:

الف- درستی‌سنجی این موضوع که ONF و فرایند مدیریت مربوط به آن سازگار با جهت راهبردی، اهداف امنیت اطلاعات و خط‌مشی سازمان است و

ب- درستی‌سنجی این موضوع که ONF با معماری سازمانی موجود سازمان همسو بوده و از آن حمایت می‌کند.

هنگامی که عناصر ONF در حوزه تکرار جاری به درستی طراحی شوند، ممیزین ممکن است معیارهایی مانند موارد زیر را در نظر بگیرند:

الف- تعریف هدف و دامنه کاربرد و راهبرد پیاده‌سازی تکرار جاری فرایند مدیریت ONF.

ب- تعریف وضعیت، اولویت‌ها و طرح‌های امنیت برنامه کاربردی راهبردی سازمان.

پ- ایجاد خط‌مشی مدیریت امنیت برنامه کاربردی.

ت- طبقه‌بندی به لحاظ امنیت و موجودی اطلاعات (یعنی واژه‌های محرمانگی، یکپارچگی و در دسترس بودن) مربوط به کاربردهای یکپارچه با معماری اطلاعات سازمان.

ث- تعریف نقش‌های پروژه برای پیاده‌سازی هر مولفه و فرایند در چارچوب ONF.

ج- تخصیص افراد به چنین نقش‌هایی.

چ- نتایج به‌دست آمده از پایش پروژه‌ها و

ح- سازوکارهای برقراری ارتباط و گزارش‌گیری.

۵-۴-۵ پیاده‌سازی ONF

۱-۵-۴-۵ مقصود

مقصود این فرایند، پیاده‌سازی عناصر ONF است که در تکرار جاری فرایند مدیریت ONF طراحی شده‌اند و راه‌حل‌هایی را در زمینه امنیت برنامه کاربردی از جمله مولفه‌ها و فرایندها ارائه می‌دهند و آن‌ها را در سراسر سازمان به‌عنوان راهنما، خدمات یا شیوه‌های اجباری مورد استفاده قرار می‌دهند.

۲-۵-۴-۵ نتایج

به‌عنوان نتیجه عملکرد موفق این فرایند، عناصر ONF توسعه‌یافته و پیاده‌سازی می‌شوند و آموزش مربوط برای بازیگران مرتبط با کاربرد عناصر ONF ارائه می‌شود.

۳-۵-۴-۵ فعالیت‌های تحقق

جدول ۷- نمودار RACI مربوط به تحقق فرایند «پیاده‌سازی ONF»

فعالیت‌های تحقق	کارگروه ONF	گروه توسعه عنصر ONF	کارشناسان حوزه
الف- تحلیل تأثیر و پیچیدگی توسعه و پیاده‌سازی عنصر ONF طراحی شده در حوزه و دامنه تکرار فرایند مدیریت جاری ONF	A/R		C
ب- برای هر عنصر طراحی شده ONF : ۱- تخصیص گروه توسعه؛	A/R		
۲- ابلاغ اهداف مدیریت و هدایت به گروه توسعه؛	A/R		
۳- فراهم کردن منابع کافی برای گروه توسعه؛	A/R		
۴- توسعه و پیاده‌سازی عنصر ONF؛	A	R	C
۵- تعیین آموزش کاربرد عنصر ONF توسط بازیگران مختلف و		A/R	C
۶- تدارک آموزش کافی برای بازیگران.	A/R	C	C

۵-۴-۵-۴ فعالیت‌های درستی‌سنجی

جدول ۸- نمودار RACI برای درستی‌سنجی فرایند «پیاده‌سازی ONF»

فعالیت‌های درستی‌سنجی	کارگروه ONF	ممیزین	کارشناسان حوزه
۱- درستی‌سنجی اینکه عناصر طراحی شده ONF مطابق با نتایج فرایند طراحی ONF توسعه یافته و پیاده‌سازی شده‌اند.	A	R	C
۲- درستی‌سنجی اینکه آموزش شناسایی شده توسط گروه توسعه عنصر ONF برای بازیگران مربوط فراهم شده است	A	R	C

۵-۴-۵-۵ راهنما

ورودی‌های پیش‌نیاز مورد استفاده در این فرایند به شرح توصیه می‌شوند:

الف- راهبرد پیاده‌سازی ONF برای تکرار جاری فرایند مدیریت ONF و

ب- طراحی عناصر ONF برای تکرار جاری فرایند.

در جایی که سازمان برون‌سپاری یا تأمین هر عنصری از ONF را انتخاب می‌کند که بر تطابق با نیازها تأثیر می‌گذارد، توصیه می‌شود نیازهای مدیریت کارگروه ONF برای ابلاغ و پیاده‌سازی توسط این هستارها از این نظر تضمین شود که کدامین عناصر برون‌سپاری شده‌اند یا از کجا تأمین می‌شوند.

هنگام تخصیص گروه توسعه به پیاده‌سازی جز ONF، به کارگروه ONF توصیه می‌شود که منابع و تخصص مورد نیاز، بالأخص به شکل کارشناسان حوزه را برای دامنه خاصی که عنصر ONF برای آن دامنه به‌کار می‌رود، در دسترس گروه قرار دهند.

مثال- کارشناسان حقوقی[1]، کارشناسان پزشکی قانونی[2]، کارشناسان فناوری[3]، کارشناسان رمزنگاری[4]، کارشناسان حریم خصوصی[5].

هنگام درستی‌سنجی، عناصر طراحی شده ONF توسعه یافته و پیاده‌سازی می‌شوند، ممیزها ممکن است معیارهایی مانند موارد زیر را در نظر بگیرند:

الف- مدیریت پروژه‌های ONF و سرمایه‌گذاری‌های صورت گرفته روی امنیت برنامه کاربردی.

ب- ایجاد سازوکارهای گزارش‌گیری و ارتباط ONF.

پ- استفاده از واسطها در پروژه‌های امنیت برنامه کاربردی برای دستیابی به عناصر ONF.

ت- ابلاغ اهمیت مدیریت موثر امنیت برنامه کاربردی، مطابق با سامانه مدیریت امنیت اطلاعات در سازمان.

1 - Legal Experts
2 - Forensic Experts
3 - Technology Experts
4 - Cryptography Experts
5 - Privacy Experts

ث- مستندسازی و ابلاغ اطلاعات طبق تعریف در استاندارد ISO/IEC 27001: 2013.

ج- پیاده‌سازی عناصر ONF برای همه کاربردهای بحرانی بسته به راهبرد پیاده‌سازی ONF و

چ- پاسخگویی هر فردی در ارتباط با پیاده‌سازی و کاربرد ONF.

علاوه بر این، ممیزها نسبت به هر عنصر طراحی شده ONF ممکن است معیارهایی مانند موارد زیر را در نظر بگیرند:

الف- شناسایی مالک.

ب- اهداف و جهت‌گیری مدیریت.

پ- صلاحیت اشخاص نسبت به انجام کار.

ت- آموزش استفاده از عناصر ONF از طریق بازیگران مختلف و

ث- پیاده‌سازی و مدیریت عناصر ONF.

راهنمای خاص برای پیاده‌سازی برخی عناصر ONF در زیربند ۵-۵ یافت می‌شود.

۵-۴-۶ پایش و بازنگری ONF

۵-۴-۶-۱ مقصود

مقصود این فرایند، بازنگری مولفه‌ها و فرایندهای ONF برای تضمین این موضوع است که برای تحقق هدف به حد کافی در نظر گرفته شده و در تطابق با خط‌مشی امنیت برنامه کاربردی استفاده می‌شوند.

۵-۴-۶-۲ نتایج

نتیجه عملکرد موفقیت‌آمیز این فرایند عبارت است از :

الف- اطلاعات مستندسازی شده به‌عنوان شاهدی بر نتایج بازنگری‌ها و

ب- شناخت و ثبت بهبودهای مورد نیاز عناصر ONF.

۵-۴-۶-۳ فعالیت‌های تحقق

جدول ۹- نمودار RACI برای تحقق فرایند «پایش و بازنگری ONF»

فعالیت‌های تحقق	کارگروه ONF	کارشناسان حوزه
۱- تعریف روش‌های استاندارد برای اندازه‌گیری، تحلیل و ارزشیابی عناصر ONF برای تضمین نتایج معتبر و قابل تکرار	A/R	C
۲- تغییرات پایش (به راهنما مراجعه کنید).	A/R	

فعالیت‌های تحقق	کارگروه ONF	کارشناسان حوزه
۳- بازنگری عناصر ONF با استفاده از روش‌های استاندارد برای اندازه‌گیری و تحلیل و ارزشیابی برای تعیین اینکه طبق انتظار انجام می‌شوند.	A/R	C
۴- حفظ اطلاعات مستندسازی به‌عنوان شواهد نتایج بازنگری‌ها	A/R	
۵- شناسایی و ثبت بهبودهای مورد نیاز برای عناصر ONF	A/R	C
۶- ابلاغ بهبودهای مورد نیاز با گروه‌های پروژه برنامه کاربردی در صورت نیاز	A/R	

۵-۴-۶-۴ فعالیت‌های درستی‌سنجی

جدول ۱۰- نمودار RACI مربوط به درستی‌سنجی فرایند «پایش و بازنگری ONF»

فعالیت‌های درستی‌سنجی	کارگروه ONF	ممیزین
۱- درستی‌سنجی هستار و کیفیت اطلاعات مستندسازی شده که به‌عنوان شواهد نتایج بازنگری‌ها ثبت می‌شود.	A	R
۲- درستی‌سنجی هستار و کیفیت اطلاعات ثبت شده در مورد بهبودهای مورد نیاز در قبال عناصر ONF.	A	R

۵-۴-۶-۵ راهنما

در مورد پایش و بازنگری، توصیه می‌شود که در فواصل زمانی طراحی شده یا در واکنش به تغییر خاصی در زمینه سازمان، برای تضمین تداوم مناسب بودن، کفایت و اثربخشی انجام گیرند.

موارد ممکن است به‌عنوان ورودی‌هایی برای این فرایند استفاده شوند:

الف- نتایج فرایند ارزیابی مخاطره امنیت اطلاعات در سازمان.

ب- تغییرات در محتواهای ONF سازمان.

پ- نتایج ممیزی‌های ONF.

ت- کسب بازخورد از سوی طرفین ذینفع.

ث- وضعیت اقدامات پیشگیرانه و اصلاحی.

ج- نتایج اکتسابی از اندازه‌گیری‌های اثربخش و

چ- سوابق حوادث در زمینه امنیت برنامه کاربردی.

بازخورد به‌دست آمده از پروژه‌های کاربردی باید به‌عنوان ورودی مهم- با توجه به بهبود مستمر کیفیت و اثربخشی ASC استقراریافته در پروژه‌ها- استفاده شود.

مثال ۱- ارزش «هزینه» تخصیص‌یافته به ASC به طور نوعی در اولین مرتبه ارزشیابی تقریبی صورت گرفته و از طریق

بازخورد کسب شده از پروژه‌ها بهتر تعریف می‌شود.

مثال ۲- با تغییرات مداوم در زمینه فناورانه سازمان، دیگر برخی از ASC ها، الزامات امنیتی پروژه‌های کاربردی جدید را برآورده نخواهند کرد. آن‌ها در نهایت قدیمی شده و از بانک ASC سازمان حذف می‌شوند. این قضیه به پیشگیری از موقعیت کنترل منسوخ برای اثر آسیب‌پذیری آن، کمک شایانی خواهد کرد.

عناصر پایش شده ONF شامل مصنوعات پروژه‌های کاربردی می‌شوند. از طریق پایش این عناصر، کارگروه ONF تضمین می‌کند که همه پروژه‌های کاربردی به نحو صحیحی از ASMP به خصوص از موارد زیر تبعیت خواهد کرد:

الف- استفاده صحیح از مولفه‌های ONF؛

ب- ایجاد سطح اعتماد مورد هدف و سطح واقعی اعتماد و

پ- انجام ارزشیابی مخاطره برنامه کاربردی دوره‌ای.

هنگام پایش و بازنگری عنصر ONF، به کارگروه ONF توصیه می‌شود که منابع و تخصص لازم، بالأخص به شکل کارشناسان حوزه را برای دامنه خاصی که عنصر ONF برای آن دامنه به‌کار می‌رود، به‌دست آورند.

مثال- کارشناسان قانونی، کارشناسان پزشکی قانونی، کارشناسان فناوری، کارشناسان رمزنگاری، کارشناسان حریم خصوصی.

هنگام درستی‌سنجی این موضوع که فرایند پایش و بازنگری ONF به درستی انجام شده، ممیزین ممکن است معیارهایی به شرح زیر را در نظر بگیرند:

الف- روش‌های تعریف و اعتباربخشی برای پایش، اندازه‌گیری، تحلیل و ارزیابی برای تضمین کسب نتایج معتبر؛

ب- شمول تصمیم‌گیری‌های مربوط به فرصت‌های بهبود مستمر و نیازهای ممکن برای تغییرات نسبت به ONF؛

پ- اطلاعات مستندسازی به‌عنوان شواهدی بر نتایج مربوط به بازنگری‌ها؛

ت- اندازه‌گیری و پایش عناصر ONF و

ث- ارزشیابی اینکه آیا اقدامات موثر هستند یا خیر.

۵-۴-۷ بهبود ONF

۵-۴-۷-۱ مقصود

مقصود از این فرایند عبارت است از:

الف- بهبود قابلیت استفاده، تناسب، کفایت و اثربخشی ONF؛

ب- افزودن عناصر مورد نیاز از دست رفته از طریق تغییرات در محیط سازمان و

پ- حفظ همسویی ONF با سامانه مدیریت امنیت اطلاعات در سازمان.

۵-۴-۷-۲ نتایج

نتیجه عملکرد موفق این فرایند به شرح زیر است:

الف- عناصر ONF بهبود می‌یابند؛

ب- نیاز به طراحی مجدد عناصر ONF بوده یا طراحی تازه عناصر ONF مستندسازی می‌شود و

پ- تغییرات صورت گرفته در مورد عناصر ONF ثبت شده، به‌طور کامل مستندسازی شده و ابلاغ می‌شود.

۵-۴-۷-۳ فعالیت‌های تحقق

جدول ۱۱- نمودار RACI برای تحقق فرایند «بهبود ONF»

فعالیت‌های تحقق	کارگروه ONF	گروه توسعه عنصر ONF	کارشناسان حوزه
۱- انجام بهبودهای مورد نیاز شناسایی شده از قبل در مورد عناصر ONF	A	R	C
۲- ارزشیابی نیاز برای طراحی مجدد عناصر ONF یا طراحی جدید عناصر ONF	A	R	C
۳- مستندسازی چنین نیازهایی و ابلاغ آن‌ها به فرایند «طراحی ONF»	A	R	C
۴- مدیریت تغییرات از طریق انجام فرایندهای سازمان مانند مدیریت تغییر، مدیریت پیکربندی و غیره	A/R		
۵- تضمین بهبود اطلاعات مانند مقصود، اهداف، الزامات امنیتی تعیین شده، توصیف و درستی‌سنجی معیارها به نحو مناسبی مستندسازی شده و ابلاغ می‌شود.	A/R		

۵-۴-۷-۴ فعالیت‌های درستی‌سنجی

جدول ۱۲- نمودار RACI برای درستی‌سنجی فرایند «بهبود ONF»

فعالیت‌های درستی‌سنجی	کارگروه ONF	ممیزین
۱- درستی‌سنجی این موضوع که بهبودهای مورد نیاز شناسایی شده از قبل در مورد عناصر ONF انجام پذیرفته‌اند.	A	R
۲- درستی‌سنجی اینکه هرگونه نیاز برای بازطراحی عناصر ONF یا طراحی عناصر جدید ONF مستند می‌شوند.	A	R
۳- درستی‌سنجی این موضوع که تغییرات نسبت به عناصر ONF ثبت شده، به نحو مناسبی مستندسازی شده و ابلاغ می‌شوند.	A	R
۴- درستی‌سنجی این موضوع که تغییرات به نحو کاملی توسط انجام فرایندهای سازمانی مانند مدیریت تغییر، مدیریت پیکربندی و غیره مدیریت شده‌اند.	A	R

۵-۴-۷-۵ راهنما

سازمان، ممکن است از فرایندهای سامانه مدیریت امنیت اطلاعات مانند رهبری، طرح‌ریزی و ارزیابی عملکرد برای دستیابی به بهبود در این موارد استفاده کند.

نتایج فرایند «پایش و بازنگری ONF» ممکن است به‌عنوان ورودی برای این فرایند، مانند موارد زیر، استفاده شود:

الف- ثبت اطلاعات مستندسازی شده به‌عنوان شاهدی بر نتایج بازنگری و

ب- اطلاعات ثبت شده در مورد بهبودهای مورد نیاز نسبت به عناصر ONF.

برای بهبود عنصری از ONF، به کارگروه ONF توصیه می‌شود که منابع و تخصص مورد نیاز، بالأخص به شکل کارشناسان حوزه را برای دامنه خاصی که عنصر ONF برای آن دامنه به‌کار می‌رود، بدست آورند.

مثال- کارشناسان قانونی، کارشناسان پزشکی قانونی، کارشناسان فناوری، کارشناسان رمزنگاری، کارشناسان حریم خصوصی.

هنگام درستی‌سنجی این موضوع که بهبود فرایند به درستی صورت گرفته است، ممیزین ممکن است معیارهای زیر را در نظر بگیرند:

الف- ارزیابی نیاز به طرح اقدامات برای تشخیص مخاطره‌ها و فرصت‌ها؛

ب- یکپارچگی و پیاده‌سازی این اقدامات در ONF، در صورت کاربردپذیری؛

پ- شناخت فرصت‌ها برای بهبود؛

ت- تغییر مدیریت و

ث- قابلیت دسترسی به بهبود اطلاعات مانند مقصود، اهداف، الزامات امنیتی مشخص شده، توصیف و تایید معیارها.

۵-۴-۸ ممیزی ONF

۵-۴-۸-۱ مقصود

مقصود از این فرایند اندازه‌گیری تطابق ONF با الزامات امنیتی برنامه کاربردی سازمان خصوصاً خط‌مشی مدیریت امنیت برنامه کاربردی سازمان است. این مورد خصوصاً برای برخی سازمان‌ها مفید است که ناگزیر هستند تضمین کنند ONF مطابق با الزامات ONF دیگری مانند ONF سازمان مادر یا ONF سازمان مقررات است.

مثال- ممکن است دولتی ONF را با کمینه الزامات در نظر گرفته شده برای همه نمایندگی‌های دولتی پیاده‌سازی کند. ONF نمایندگی ناگزیر به تطابق با ONF دولتی یعنی ناگزیر به پیاده‌سازی کمینه الزامات در ONF دولت است. این تطابق ممکن است طی ممیزی ONF نمایندگی تایید شود.

۵-۴-۸-۲ نتایج

در نتیجه عملکرد موفق این فرایند:

الف- برنامه ممیزی ONF پیاده‌سازی و مدیریت می‌شود؛

ب- عناصر ONF مطابق با برنامه ممیزی می‌شود؛

پ- نتایج ممیزی به‌طور کامل مستندسازی شده و ابلاغ می‌شود و

ت- نتایج ممیزی برای بهبود مستمر ONF به کار گرفته می‌شود.

۵-۴-۸-۳ فعالیت‌های تحقق

جدول ۱۳- نمودار RACI مربوط به تحقق فرایند « ممیزی ONF »

فعالیت‌های تحقق	مدیران	ممیزین	کارگروه ONF	کارشناسان حوزه
۱- پیاده‌سازی و مدیریت برنامه ممیزی ONF برای یکپارچگی فعالیت‌های ممیزی ONF با فرایندهای ممیزی موجود.	A	R	C	C
۲- تضمین این موضوع که ممیزین، آموزش کافی را برای ممیزی ONF دریافت می‌کنند.	A/R			C
۳- ممیزی ONF.	A	R	C	C
۴- یافتن علل ریشه‌ای عدم انطباق و راه‌حل‌های پیشنهادی در نتایج ممیزی.	I	A	C	R
۵- مستندسازی و ابلاغ نتایج ممیزی.	A	R	I	
۶- تضمین این موضوع که نتایج ممیزی به‌عنوان ورودی فرایند پایش و بازنگری ONF فراهم شده‌اند.		A/R	C	

۵-۴-۸-۴ فعالیت‌های درستی‌سنجی

جدول ۱۴- نمودار RACI مربوط به درستی‌سنجی فرایند «ممیزی ONF»

فعالیت‌های درستی‌سنجی	مدیران	ممیزین بیرونی
۱- درستی‌سنجی اینکه فعالیت‌های ممیزی ONF مطابق با برنامه ممیزی ONF هستند.	A	R

۵-۸-۴-۵ راهنما

توصیه می‌شود مدیریت مناسب پاسخگوی، برنامه ممیزی ONF را پیاده‌سازی و مدیریت کرده، ممیزین را هدایت کرده و علاوه بر راهنمای گنجانده شده در استاندارد ISO/IEC 27007 صلاحیت ممیزین را تضمین کند.

در پیاده‌سازی برنامه ممیزی ONF، به مدیریت توصیه می‌شود فرایندهای ممیزی موجود سازمان خصوصاً فرایند ممیزی سامانه مدیریت امنیت اطلاعات را چنانچه پیاده‌سازی شده باشد، بازنگری کند و راهبردی را با فرایند ممیزی ONF نظیر فرایندهای موجود، همسو و یکپارچه کند. به مدیریت توصیه می‌شود که اصول راهنمایی را برای ممیزی سامانه‌های مدیریت مطابق زیربند ۵-۲-۱ از استاندارد ISO 19011:2011 در نظر بگیرد.

به کارگروه ONF توصیه می‌شود تعیین کند که چه اجزای خاصی از ONF لازم است ممیزی شده و چه فعالیت‌هایی نیاز است به فرایند ممیزی موجود به منظور برآوردن اهداف تنظیمی توسط مدیریت در برنامه ممیزی اضافه شود.

برنامه ممیزی ONF نه تنها به تایید مدیریت مناسب پاسخگو نیاز دارد، بلکه به منابع و استقلالی نیاز دارد که به لحاظ عینی نشان دهند ONF الزامات امنیت برنامه کاربردی سازمان را به شرح زیر برآورده می‌کند:

الف- مسئولیت‌ها به وضوح در نمودارهای RACI (به روش‌های مشابهی) تعریف و ابلاغ می‌شوند؛

ب- عناصر ONF مقرون به صرفه و به‌روزرسانی می‌شوند؛

پ- تغییر فرایندهای مدیریت دنبال می‌شوند؛

ت- فرایندهای فرعی مدیریت تکمیل می‌شوند؛

ث- فعالیت‌های درستی‌سنجی هر زیرفرایند مدیریت ONF صورت می‌گیرد و

ج- نتایج ممیزی گذشته و ارزشیابی مخاطره در نظر گرفته می‌شوند.

توصیه می‌شود ورودی‌های پیش‌نیاز برای این فرایند به شرح زیر استفاده شوند:

الف- نتایج ممیزی گذشته و ارزشیابی مخاطره و

ب- درخواست‌های فراهم آمده طبق سامانه مدیریت امنیت اطلاعات.

هنگام ممیزی ONF، به کارگروه ONF توصیه می‌شود که منابع و تخصص مورد نیاز، بالأخص به شکل کارشناسان حوزه را برای دامنه خاصی که عناصر ONF برای آن دامنه به‌کار می‌روند، به‌دست آورند.

مثال: کارشناسان قانونی، کارشناسان پزشکی قانونی، کارشناسان فناوری اطلاعات، کارشناسان رمزنگاری ، کارشناسان حریم خصوصی.

به ممیزین بیرون از سازمان با الزام مدیریت مناسب پاسخگو توصیه می‌شود که فرایند ممیزی ONF را با در نظر گرفتن موارد زیر انجام دهند:

الف- ایجاد برنامه ممیزی؛

ب- تایید برنامه ممیزی و بازنگری منابع؛

پ- نتایج گزارش شده در مورد فرایند ممیزی ONF؛

ت- فهرستی از عوامل ریشه‌ای عدم انطباق‌ها و راه‌حل‌ها؛

ث- شواهدی مبنی بر پایش راه‌حل‌ها و

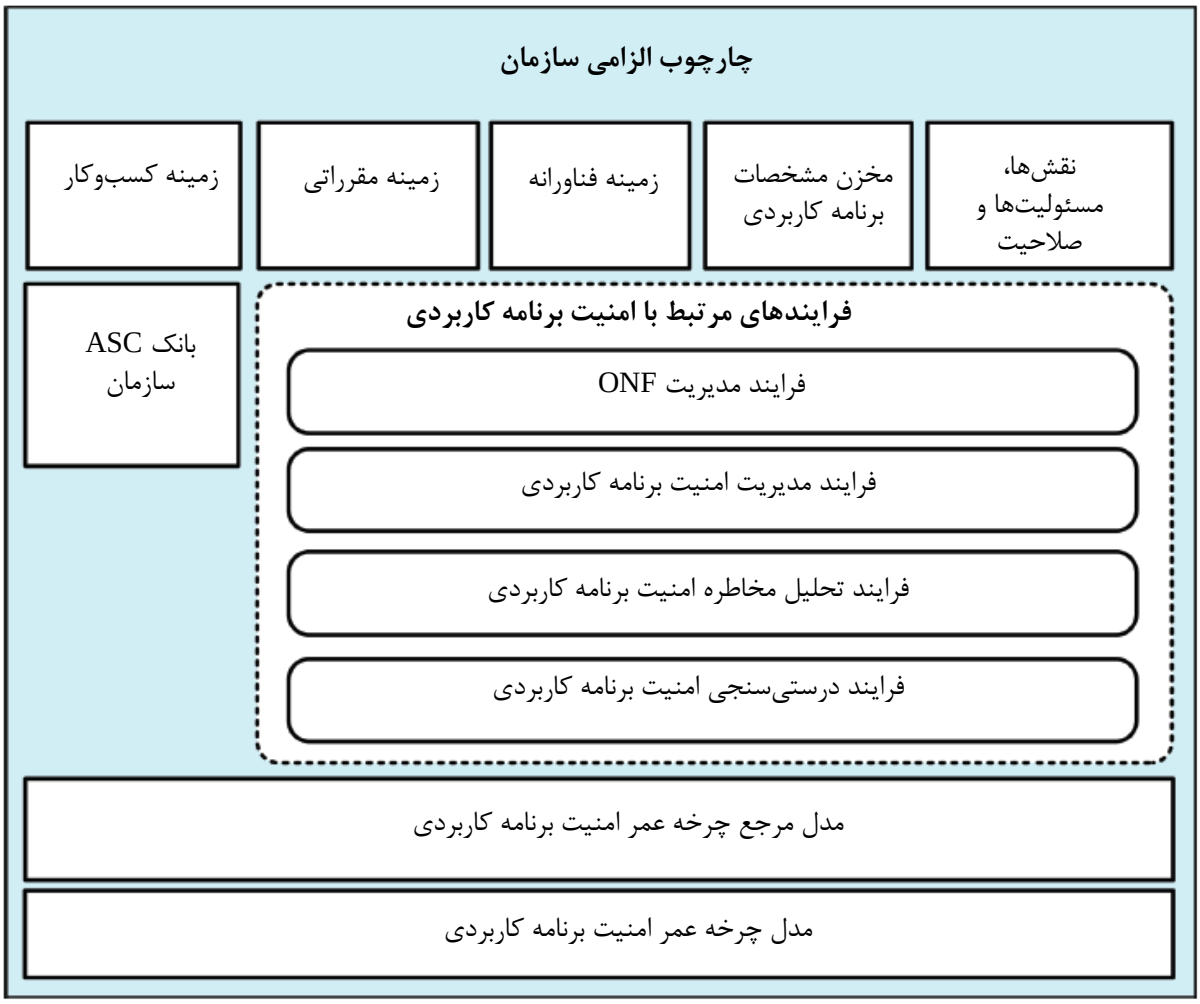
ج- بهبود فرایند ممیزی

یادآوری- ممیزین مذکور ممکن است بیرون یا داخل سازمان باشند ولی توصیه می‌شود خارج از هدف و دامنه امنیت برنامه کاربردی در سازمان و خارج از حیطه اقتدار کارگروه ONF قرار گیرند. همانند هر فرایندی، توصیه می‌شود تفکیک در محدودیت وظیفه بین فعالیت‌های تحقق و درستی‌سنجی آن‌ها برای این فرایند در نظر گرفته شود.

۵-۵ عناصر ONF

۵-۵-۱ کلیات

چارچوب ONF عناصری مانند مولفه‌ها و فرایندهایی را برای پرداختن به الزامات امنیت برنامه کاربردی سازمان فراهم می‌آورد. نمایش نگاشتاری ساده محتوای ONF طبق شکل ۲ ارائه می‌شود.



شکل ۲- چارچوب الزامی سازمان – بازنمایی ساده‌شده نگاشتاری

یادآوری- دو نوع از عناصر در این استاندارد تعریف می‌شوند: مولفه‌ها و فرایندها. مولفه‌ها طبق شکل ۲ با استفاده جعبه‌های مربع شکل و فرایندها از طریق جعبه‌های مدور نمایش داده می‌شوند.

۵-۵-۲ مولفه زمینه کسب‌وکار

۵-۵-۲-۱ مقصود

این مولفه به شناسایی مخاطره‌های امنیتی و الزامات نشات گرفته از فعالیت‌های کسب‌وکار سازمان کمک می‌کند و مقادیری را فراهم می‌آورد که در خصوصیت رسیدگی به الزامات ASC مورد ارجاع قرار می‌گیرد. این مولفه رویکرد استاندارد تایید شده‌ای را برای کاهش مخاطره‌های در ارتباط با دامنه کسب‌وکار سازمان معرفی می‌کند.

۵-۵-۲-۲ توصیف

زمینه کسب‌وکار فهرست و مستنداتی از همه فرایندهای کسب‌وکار، استانداردها و بهترین روش‌های پذیرفته شده توسط سازمان است که می‌تواند دارای تأثیری بر پروژه‌های برنامه کاربردی باشد. چنین فعالیت‌هایی موجب ایجاد مخاطرات شده و به سازمان توصیه می‌شود الزامات امنیتی را برای کاهش این مخاطرات تعیین کند. توصیه می‌شود ASCها در جایگاهی برای رفع الزامات قرار داده شوند. سازندگان ASC نیاز به تشخیص این موضوع دارند که چرا ASC فراهم می‌شود یعنی ASC بر اساس کدام الزامات امنیتی پیاده‌سازی می‌شود. آن‌ها اطلاعات مورد نیاز در مولفه زمینه کسب‌وکار ONF را پیدا خواهند کرد.

مثال ۱- خط‌مشی امنیتی سازمان به‌طور عادی منبع مستقیم الزامات امنیتی است. برخی از آن‌ها مربوط به امنیت کاربردی می‌شوند. عدم انطباق با خط‌مشی امنیتی مخاطره‌ای است که مالک برنامه‌ای کاربردی معمولا یارای تحمل آن را ندارد. ASCها ممکن است برای برآوردن الزامات خاصی از خط‌مشی امنیتی طراحی شوند.

مثال ۲- فرایند کسب‌وکار برای تولید هواپیما در دامنه کسب‌وکار حمل‌ونقل هوایی به سطح بالایی از مخاطره و متعاقبا الزامات امنیتی متعدد آورده می‌شود. در نتیجه، ASCهای متعدد معمولا به برنامه‌های کاربردی مرتبط با این فرایند اضافه خواهند شد.

۵-۵-۲-۳ مندرجات

توصیه می‌شود زمینه کسب‌وکار موارد را فراهم آورد:

الف- فهرست همه دامنه‌های کسب‌وکار مربوط به همه قسمت‌های سازمان که برنامه‌های کاربردی در آن اجرا شده یا استفاده خواهند شد؛

ب- فهرستی از فرایندها، خط‌مشی‌ها و بهترین شیوه‌ها، برای هر دامنه کسب‌وکار که مربوط به کاربرد برنامه‌های کاربردی در دامنه مربوط می‌شوند، مانند:

۱- کسب‌وکار، مدیریت پروژه، توسعه، تحلیل مخاطره، عملیاتی، ممیزی و کنترل و فرایندهای مدیریت تغییر.

۲- خط‌مشی امنیتی سازمان.

۳- فهرستی از دارایی‌های اطلاعاتی سازمان همراه با طبقه‌بندی امنیتی آن‌ها.

۴- توسعه روش‌های مورد استفاده سازمان.

۵- بهترین شیوه‌ها برای همه زبان‌های برنامه‌نویسی به‌کار گرفته شده توسط سازمان و فهرست شده در زمینه سازمان و

۶- استانداردها مانند استانداردهای بین‌المللی ISO/IEC و استانداردهای صنعتی که سازمان ملزم به پیروی از آن‌ها است.

پ- فهرستی از مخاطرات ایجاد شده توسط فرایندها، خط‌مشی‌ها و بهترین شیوه‌های فوق که مربوط به امنیت برنامه کاربردی می‌شوند؛

ت- فهرستی از الزامات امنیتی برای کاهش مخاطرات فوق؛

ث- راهنما و اصول راهنمایی برای توسعه ASC شامل:

۱- فهرستی از خصوصیات ASC که ممکن است برای توصیف مورد ASC به کار برده شوند.

۲- تطبیق با خصوصیات توصیف شده در استاندارد ISO/IEC 27034-5 و

۳- در صورت کاربردپذیری، برای هر ویژگی، مجموعه‌ای از مقادیر مجاز، قواعد، کوته‌نوشت‌ها و وابستگی‌ها.

۵-۵-۲-۴ راهنما

توصیه می‌شود اطلاعات مورد نیاز برای ایجاد مولفه ONF مذکور از طریق تحلیل مخاطره امنیت اطلاعات به‌دست آید. در مورد سازمان‌هایی که تحلیل مخاطره امنیت اطلاعات را انجام داده‌اند به تبعیت از اصول راهنمای استاندارد ISO/IEC 27001: 2003 و در انطباق با فرایند مدیریت مخاطره ارائه شده در استاندارد ملی ایران شماره ۲۷۰۰۵، توصیه می‌شود تلاش مورد نیاز برای ایجاد مولفه کمینه باشد.

توصیه می‌شود فهرستی از دارایی‌های اطلاعات سازمان با طبقه‌بندی امنیتی، از طریق معماری اطلاعات سازمان تامین شوند. این قضیه اشاره به موجودی دارایی‌ها در استاندارد ISO/IEC 27001: 2013,A.8.1.1 دارد.

توصیه می‌شود فهرست دارایی‌های اطلاعات سازمان برای مدیریت کارآمد مخاطره دانه‌درشتیِ کافی را داشته باشد. به ندرت حالتی روی می‌دهد که همه اطلاعات مورد استفاده برنامه کاربردی دارای طبقه‌بندی امنیتی یکسان باشند. طبقه‌بندی گروه‌های اطلاعات در داخل دارایی بسیار کارآمدتر است.

مثال- دارایی اطلاعات ممکن است از هزاران جدول تشکیل شود که تنها تعداد کمی از آن‌ها شامل اطلاعات محرمانه هستند.

توصیه می‌شود فهرستی از الزامات امنیتی در این مولفه به حدی خاص در نظر گرفته شود که مستقیماً برای طرح‌ریزی، طراحی و پیاده‌سازی ASCها مفید واقع شود.

سازمان به افزودن راهنما و اصول راهنما برای توسعه ASC نیاز دارد زیرا ممکن است تصمیم به پیاده‌سازی مجموعه کاملی از خصوصیت‌های ASC توصیفی در استاندارد ISO/IEC 27034-5 یا زیرمجموعه یا زیرمجموعه‌هایی از آن گرفته شود یا با نیازها یا الزامات مستند موجود برای کنترل امنیتی تطابق یابد.

با وجود اینکه سازمان راهنما و اصول راهنمای ASC را تعریف می‌کند، توصیه می‌شود این موارد کمینه الزامات برشمرده در استاندارد ISO/IEC 27034-5 را برآورده کند.

برای تضمین سازگاری، به کارگروه ONF توصیه می‌شود، اطمینان حاصل کند که راهنما و اصول راهنمای ASC ایجاد شده و در دسترس گروه‌های توسعه ASC در تکرارهای اولیه فرایند مدیریت ONF قرار گیرد. فرایند مدیریت ONF امکان تکامل راهنما و اصول راهنمای ASC را طی زمان فراهم می‌آورد.

۵-۵-۳ مولفه زمینه مقرراتی

۵-۵-۳-۱ مقصود

این مولفه به تعیین مخاطره‌های امنیتی ناشی از زمینه مقرراتی سازمان خصوصاً مخاطره‌هایی که ناشی از شکست سازمان در تطابق با قوانین و مقررات مربوط است، کمک می‌کند. این مؤلفه، مقادیری را تامین می‌کند که در خصوصیت الزامات مشخص شده ASC به آن‌ها ارجاع می‌شود. همچنین رویکرد استاندارد تایید شده برای کاهش مخاطرات در ارتباط با هر قاعده یا مقرراتی را معرفی می‌کند.

۵-۵-۳-۲ توصیف

زمینه مقرراتی، فهرست و سندی از قوانین و مقررات است که می‌تواند بر پروژه‌های برنامه کاربردی در هر موقعیت کسب‌وکار سازمان، یعنی در کشورها یا حوزه‌های قضایی که برنامه کاربردی در آن توسعه داده شده، استقرار یافته یا استفاده می‌شود، تأثیر داشته باشد.

این فهرست خصوصاً برای تعیین قوانین و مقرراتی مفید خواهد بود که به مشخصات برنامه کاربردی مرتبط با فعالیت‌های کسب‌وکار مربوط می‌شود. توصیه می‌شود اطلاعات اضافی به فهرستی برای این هدف اضافه شود.

۵-۵-۳-۳ مندرجات

توصیه می‌شود زمینه مقرراتی موارد زیر را فراهم آورد:

الف- فهرستی از قوانین و مقرراتی که مطابق با موقعیتی که برنامه‌های کاربردی برای/به‌وسیله سازمان استفاده خواهند شد، کاربردپذیر هستند.

ب- فهرستی از مخاطرات ایجاد شده توسط قوانین و مقررات که به امنیت برنامه کاربردی مربوط می‌شود.

پ- فهرستی از الزامات امنیتی برای کاهش مخاطرات فوق.

۵-۵-۳-۴ راهنما

توصیه می‌شود اطلاعاتی برای ایجاد مولفه ONF از طریق تحلیل مخاطره امنیتی کسب شود. برای سازمان‌هایی که تحلیل مخاطره امنیت اطلاعات را به پیروی از راهنمای استاندارد ISO/IEC 27001:2013 و در انطباق با فرایند مدیریت مخاطره ارائه شده در استاندارد ISO/IEC 27005: 2011 اجرا کرده‌اند، کمینه تلاش مورد نیاز برای ایجاد مولفه مذکور توصیه می‌شود.

توصیه می‌شود فهرستی از الزامات امنیتی در این مولفه به حدی خاص باشد که مستقیما برای طرح‌ریزی، طراحی و پیاده‌سازی ASC مفید واقع شود.

توصیه می‌شود سازمان به ایجاد فهرست کامل و کافی از قوانین و مقرراتی که مطابق با موقعیتی که برنامه‌های کاربردی برای سازمان یا توسط آن استفاده خواهند شد، توجه خاصی مبذول کند (و ممکن است منابع قابل ملاحظه‌ای را اختصاص دهد). قوانین و مقررات برای هر کشوری که برنامه کاربردی در آنجا طراحی، توسعه، کسب، تامین، استفاده و مورد عملیات قرار می‌گیرد، کاربردپذیر خواهند بود.

پیچیدگی معماری، مانند حالتی که در برنامه‌های کاربردی توزیع‌یافته یا ابری وجود دارد، ممکن است با این مسئله آمیخته شود. در معماری توزیع‌یافته، مولفه‌های رابط کاربری برای پردازش و ذخیره داده‌ها، ممکن است به لحاظ فیزیکی در کشورهای متفاوتی قرار گرفته و منوط به قواعد مختلفی شوند.

بنابراین به سازمان توصیه می‌شود به کمک کارشناسان قانونی:

الف- مغایرت‌های احتمالی در قوانین چندگانه و نیازهای الزامی را رفع کند و

ب- الزامات قانونی را به ASCها ترجمه کند.

توصیف فرایندی که چنین کاری را انجام دهد، خارج از هدف و دامنه کاربرد این استاندارد است.

یادآوری- چنین کارشناسان قانونی به‌عنوان کارشناسان حوزه در پیاده‌سازی ONF و پایش و بهبود فرایندهای ONF عمل می‌کنند(به زیربندهای ۵-۴-۵-۳ و ۵-۴-۶-۳ مراجعه شود).

۵-۵-۴ مولفه زمینه فناورانه

۵-۴-۵-۱ مقصود

این مولفه به تعیین مخاطرات امنیتی ناشی از زیرساخت فناورانه سازمان کمک می‌کند. مولفه مذکور مقادیری را فراهم می‌آورد که به خصوصیت الزامات مشخص شده ASC ارجاع می‌یابد. اطلاعاتی را در این مورد فراهم می‌آورد که چه مولفه‌های فناوری اطلاعاتی ممکن است در حمایت از ASCهایی استفاده شود که به چنین حمایتی نیاز دارند.

۵-۴-۵-۲ توصیف

زمینه فناورانه سند مولفه‌های فناوری اطلاعات سازمان (مانند مولفه‌های فیزیکی، برنامه‌های کاربردی، خدمات) و بهترین شیوه‌ها و قواعد سازمان است که برای کاربرد چنین مولفه‌هایی اعمال می‌شود.

۵-۵-۴-۳ مندرجات

توصیه می‌شود زمینه فناورانه موارد زیر را تامین کند:

الف- فهرستی از مولفه‌های فناوری اطلاعات مورد استفاده در سازمان که مربوط به امنیت برنامه‌های کاربردی است؛

ب- فهرستی از مخاطراتی که از طریق مولفه‌های فوق، به سازمان وارد می‌شود و

پ- فهرستی از الزامات امنیتی برای کاهش مخاطرات فوق.

۵-۵-۴-۴ راهنما

توصیه می‌شود اطلاعاتی برای ایجاد مولفه ONF از معماری فناورانه سازمان و از طریق تحلیل مخاطره امنیت اطلاعات به‌دست آید. برای سازمان‌هایی که تحلیل مخاطره امنیت اطلاعات را به تبعیت از اصول راهنمای استاندارد ISO/IEC 27001:2013 و در انطباق با فرایند مدیریت مخاطره ارائه شده در استاندارد ملی ایران شماره ۲۷۰۰۵، انجام می‌دهند، تلاش کمینه‌ای برای ایجاد این مولفه توصیه می‌شود.

فهرستی از الزامات امنیتی در این مولفه باید به حدی خاص در نظر گرفته شود که مستقیما در طرح‌ریزی، طراحی و پیاده‌سازی ASC مفید واقع شود.

۵-۵-۵ مخزن مشخصات برنامه کاربردی

۵-۵-۵-۱ مقصود

این مولفه به تعیین مخاطرات امنیتی ناشی از مشخصات برنامه کاربردی سازمان و کاهش مخاطره ناشی از پیاده‌سازی ناصحیح یا کاربرد نادرست این نوع مشخصات کمک می‌کند. این مولفه مقادیر را برای ارجاع به خصوصیت تحت عنوان الزامات مشخص شده مربوط به ASC فراهم می‌آورد.

۵-۵-۵-۲ توصیف

مخزن مشخصات برنامه کاربردی سندی از الزامات عملکردی فناوری اطلاعات عمومی و راه‌حل‌های مرتبط از پیش تاییدشده است. توصیه می‌شود همه مشخصات، عملکردها و خدمات در برنامه‌های کاربردی سازمان گنجانده یا ارائه شوند که شامل اسناد و بهترین شیوه‌ها برای پیاده‌سازی، کاربرد و درستی‌سنجی می‌شود.

راه‌حل‌های از پیش تاییدشده اغلب فرایندها، محصولات یا بانک[1] (بانک) کدی هستند که سازمان توصیه کرده یا شیوه الزامی را از طریق قواعد، خط‌مشی‌ها یا معماری سازمانی در محیط خاص به‌کار می‌برند. چنین راه‌حل‌هایی به‌طور عادی بالغ بوده و به‌طور مستمر بهبود می‌یابند. مزیت ارتباط ASCها با چنین راه‌حل‌هایی این است که استفاده مجدد ثابت از آن‌ها آشکار است.

1 - Library

۵-۵-۵-۳ مندرجات

توصیه می‌شود مخزن مشخصات برنامه کاربردی، موارد زیر را تامین کند:

الف- فهرستی از همه مشخصات برنامه کاربردی گنجانده شده در برنامه کاربردی سازمان یا ارائه شده توسط آن‌ها؛

ب- فهرستی از فرایندها و بهترین شیوه تایید شده توسط سازمان، برای هر مشخصه که مربوط به پیاده‌سازی، کاربرد، نگهداری یا درستی‌سنجی آن می‌شود؛

پ- فهرستی از مخاطرات ایجاد شده برای سازمان از طریق مشخصات برنامه کاربردی فوق و

ت- فهرستی از الزامات امنیتی برای کاهش مخاطرات فوق.

۵-۵-۵-۴ راهنما

توصیه می‌شود اطلاعات برای ساخت این مولفه ONF از ساختار مستند برنامه‌های کاربردی سازمان و ساختار کسب‌وکار سازمان گرفته شود.

برخی از اطلاعات ممکن است از طریق تحلیل مخاطره امنیتی حاصل شود. برای سازمان‌هایی که تحلیل مخاطره را به تبعیت از اصول راهنمای استاندارد ISO/IEC 27001: 2013 و در انطباق با فرایند مدیریت مخاطره ارائه شده در استاندارد ملی ایران شماره ۲۷۰۰۵ اجرا کرده‌اند، کمینه تلاش برای ایجاد چنین مولفه‌ای توصیه می‌شود.

توصیه می‌شود فهرستی از الزامات امنیتی در این مولفه به حد خاص در نظر گرفته شود که مستقیماً برای طرح‌ریزی، طراحی و پیاده‌سازی ASCها مفید واقع شود.

مثال- سازمان، دارای برنامه کاربردی تحت عنوان «خدمت انتقال پرونده M012» بوده و در نظر دارد همه پروژه‌های برنامه کاربردی آینده را برای کاربرد این خدمت به منظور انتقال امن اسناد بین برنامه‌های کاربردی به‌کار برد. بنابراین سازمان به ثبت این عملکرد در مخزن مشخصات برنامه کاربردی همراه با اطلاعات مرتبط مانند موارد نیاز دارد:

الف- مشخصات برنامه کاربردی، «انتقال اسناد به هستار بیرونی در برنامه کاربردی و داخلی در سازمان است»؛

ب- فهرستی از فرایندها و بهترین شیوه شامل «توصیه می‌شود در مواقع ممکن، اسناد همواره با استفاده از خدمت انتقال پرونده M012 سازمان انتقال یابند» که (این خدمت) در هستاری در زمینه فناورانه سازمان مربوط به ONF تعریف می‌شود؛

پ- فهرستی از مخاطرات شامل «نقض محرمانه بودن اسناد انتقال‌یافته بین برنامه‌های کاربردی» و

ت- فهرستی از الزامات امنیتی شامل «رمزنگاری قوی پرونده[1]ها بین نقاط انتهایی طی انتقال» و «اصالت‌سنجی کارساز و سمت سمت کارخواه».

1 - File

در دوره فرایند مدیریت ONF به سازمان توصیه می‌شود ASCهایی را ایجاد کند که به درستی الزامات امنیتی را از طریق ایجاد الزام در کاربرد خدمت انتقال پرونده M012 مشخص می‌کند. از حالا به بعد برای هر پروژه برنامه کاربردی، انتخاب این‌گونه است که ASCهای مذکور به پروژه برنامه کاربردی اضافه شود.

۵-۵-۶ نقش‌ها، مسئولیت‌ها و صلاحیت مربوط به مخزن اطلاعات

۵-۵-۶-۱ مقصود

این مولفه به تعیین مخاطرات امنیتی که از افراد مرتبط با برنامه‌های کاربردی سازمان نشات می‌گیرند، کمک می‌کند. همچنین به‌عنوان کمکی در تضمین این موضوع محسوب می‌شود که جای خالی همه نقش‌های بحرانی را برای همه فرایندها در سازمان پر کرده، همه مسئولیت‌ها را به نحوی تعریف می‌کند که از تضاد منافع اجتناب شود و افرادی به این نوع نقش‌ها تخصیص یابند که دارای صلاحیت حرفه‌ای کافی در این زمینه باشند.

۵-۵-۶-۲ توصیف

نقش‌ها، مسئولیت‌ها و صلاحیت‌های مخزن اطلاعات، مستندسازی از نقش‌ها، مسئولیت‌ها و صلاحیت‌ها در مورد بازیگران در تعامل با برنامه‌های کاربردی سازمان محسوب می‌شود.

۵-۵-۶-۳ مندرجات

توصیه می‌شود، نقش‌ها، مسئولیت‌ها و صلاحیت‌های مخزن اطلاعات موارد زیر را فراهم آورد:

الف - فهرستی از همه نقش‌های در ارتباط با برنامه‌های کاربردی سازمان؛

مثال- اپراتور برنامه کاربردی، معماری‌های برنامه کاربردی، معماری‌های امنیتی، معماری‌های فناوری، مدیر پروژه، مامور امنیتی ارشد، مالک برنامه کاربردی، توسعه‌دهندگان، مدیران، گروه زیرساخت فناوری اطلاعات، مربیان، عرضه‌کنندگان، ذینفعان، مدیر امنیتی، کارشناسان قوانین و مقررات، آزمون‌گران، کاربران

ب- فهرستی از مسئولیت‌های تخصیص‌یافته به نقش‌های فوق و

پ- فهرستی از صلاحیت‌های مورد نیاز برای انجام مسئولیت‌های فوق.

۵-۵-۶-۴ راهنما

اطلاعاتی در مورد ایجاد این مولفه ممکن است از طریق دپارتمان منابع انسانی و معماری کسب‌وکار سازمان فراهم شود.

فهرستی از صلاحیت‌های مورد نیاز در این مولفه به حدی خاص در نظر گرفته می‌شود که مستقیماً برای طرح‌ریزی، طراحی و پیاده‌سازی ASCها مفید واقع شود.

۵-۵-۷ بانک ASC مخصوص سازمان

۵-۵-۷-۱ مقصود

مولفه بانک ASC برای سازمان‌دهی ASCها مطابق با سطوح اطمینان و برای سهولت ابلاغ ASCها و انتخاب مناسب ASCها در دوره پروژه سازمانی به‌کار برده می‌شود.

۵-۵-۷-۲ توصیف

بانک ASC مخزنی از ASCهای قابل دسترس در سازمان است. هر ASC در این مخزن در ارتباط با یک یا چند سطح اطمینان است.

۵-۵-۷-۳ مندرجات

توصیه می‌شود بانک ASC موارد زیر را تامین کند:

الف- فهرستی از سطوح اطمینان مورد استفاده در سازمان شامل اطلاعاتی مانند شناسه کاربری، نام و توصیف؛

ب- فهرستی از ASCهای تخصیص یافته به هر یک از سطوح اطمینان و

پ- فهرست سلسله مراتبی از همه ASCهای نگهداری شده در ONF.

۵-۵-۷-۴ راهنما

طی دوره ایجاد بانک ASC، به سازمان توصیه می‌شود که منابعی را به شرح زیر در نظر بگیرد:

الف- موارد واپایش بر اساس فعالیت‌های ممیزی قبلی پیشنهاد می‌شود؛

ب- موارد واپایش در ارتباط با نتایج ارزیابی‌های مخاطره؛

پ- موارد واپایش به نحو وسیعی شامل بانک‌های پذیرفته شده مانند استاندارد ISO/IEC 27002,[1]، استاندارد ISO/IEC 15408 و NISTSP 800-53 می‌شود؛

ت- موارد پایش توسعه‌یافته و توسط طرف‌های سوم قابل دسترس می‌شود.

پروژه‌ها ممکن است رویکردهای افزوده خاصِ سامانه را منوط به قواعد سازمانی به‌کار برند. در مواردی که واپایش‌ها از منابع دیگر استحصال می‌شود، توصیه می‌شود به نحوی منبع شناسایی شود که بتواند همگام با تکامل سازمان، ادامه داشته باشد.

مسئولیت کارگروه ONF ایجاد بانک ASC است که اولویت‌ها و الزامات امنیتی خاص سازمان را برآورده کند.

---

۱ - استاندارد ملی ایران به شماره ۲۷۰۰۲ مربوط به سال ۲۰۰۵ موجود است.

به تبعیت از دیدگاه برنامه کاربردی محور این استاندارد، تصمیم کارگروه ONF ممکن است بر این مبنا قرار گیرد که این هدف به بهترین نحو از طریق تحلیل برنامه‌های کاربردی جدید یا موجود در سازمان به دست می‌آید و بدین ترتیب الزامات و مخاطرات امنیتی آن‌ها را تعیین کرده و ASCها را برای رفع این نیازها مطابق با اولویت‌هایی معمولا بر اساس مخاطرات پیاده‌سازی می‌کند.

به‌عنوان پیش‌نیازی برای این فعالیت، به کارگروه ONF توصیه می‌شود مولفه‌های ضروری ONF را در فرایندهای تکرار اولیه مدیریت ONF پیاده‌سازی کند.

مثال ۱- به منظور تعیین مخاطرات و اولویت‌ها، توصیه می‌شود فهرستی از دارایی‌های اطلاعات سازمان همراه با طبقه‌بندی امنیتی آن‌ها در مولفه زمینه کسب‌وکار ONF قابل دسترس شود.

توصیه می‌شود همه مولفه‌های مرتبط ONF (زمینه کسب‌وکار، زمینه مقرراتی، زمینه فناورانه، نقش‌ها، مسئولیت‌ها و مخزن صلاحیت‌ها و مخزن مشخصات برنامه کاربردی)، در تحلیل مخاطره برای ایجاد الزامات امنیتی در نظر گرفته می‌شود که منجر به توسعه ASCها می‌شود.

به‌علت ارتباط ASCها با الزامات امنیتی، ممکن است تغییر در الزامات امنیتی آغازگر تغییری در همه ASCهای مرتبط با آن شود.

با چنین ورودی ضروری در نتیجه طراحی ONF، توصیه می‌شود کارگروه ONF تعیین کند، برنامه کاربردی در تکرار بعدی فرایند مدیریت ONF مورد تحلیل قرار گیرد. برخی سازمان‌ها ممکن است برای برنامه‌های کاربردی با استفاده از دارایی‌های اطلاعاتی همراه با طبقه‌بندی امنیتی بالا اولویت قائل شوند.

برای هر برنامه کاربردی، توصیه می‌شود کارگروه ONF، ASCهایی را برای رفع نیازهای امنیتی برنامه کاربردی پیاده‌سازی کند. سپس توصیه می‌شود کارگروه ONF فرایند پیاده‌سازی ONF را برای این موارد ASC انجام دهد. به زیربند ۵-۵-۸-۳ به‌عنوان راهنمایی در مورد پیاده‌سازی ASCها مراجعه کنید.

نتیجه این پیاده‌سازی، کسب مجموعه‌ای از ASCها است که به کارگروه ONF توصیه می‌شود در بانک ASC به نحوی بگنجانند که در پروژه‌های برنامه کاربردی قابل استفاده شود.

می‌توان بانک ASC موجود را به سه طریق ممکن تطابق داد:

الف- کل مجموعه ASC که تاکنون از سطح اطمینان موجود در بانک تشکیل شده است، در حالتی که موردی به بانک اضافه نشود، ASCهای موجود به‌سادگی به‌روزرسانی می‌شوند.

ب- سطح اطمینان موجود به‌دقت با مجموعه کامل ASCها تطبیق می‌یابد، در حالتی که بانک از طریق ASCهای حاصله از مجموعه تکمیل می‌شود یا

پ- سطح جدید اطمینان از مجموعه ASCها در بانک ایجاد می‌شود.

مثال ۲- سازمانی فرایند فوق را برای اولین مرتبه انجام می‌دهد. بانک ASC خالی است. لذا کارگروه ONF تصمیم می‌گیرد مجموعه جدیدی از ASCها را به‌عنوان سطح اطمینان جدید در بانک ASC بگنجاند. این سطح اطمینان «برنامه کاربردی C2 از نوع کارخواه-کارساز بدون قرار گرفتن در معرض اینترنت» برچسب می‌خورد که «C2» طبقه‌بندی محرمانگی برای

دارایی‌های اطلاعاتی برنامه کاربردی بر مقیاسی مطرح می‌شود که از C1 الی C4 تغییر ی‌کند (C4 از بالاترین تأثیر محرمانگی و C1 از پایین‌ترین تأثیر سطح محرمانگی برخوردار است). این سطح اطمینان برای هر برنامه کاربردی مشابهی با استفاده از دارایی‌های اطلاعاتی C1 یا C2 به‌کار برده خواهد شد.

مثال ۳- همان سازمان این فرایند را مجددا برای برنامه کاربردی موجود دیگری انجام می‌دهد که مشابه با مورد مثال ۲ است البته تنها با این تفاوت که از برخی دارایی‌های C3 استفاده کرده و از کنترل امنیتی کمتری برخوردار است. از آنجا که مجموعه جدید ASCها به‌دقت با سطح اطمینان موجود تطابق می‌یابد، کارگروه ONF تصمیم می‌گیرد سطح اطمینان موجود را به‌روزرسانی کرده و آن را مجددا تحت عنوان «C3 برنامه کاربردی از نوع کارخواه-کارساز بدون در معرض قرار گرفتن اینترنت» برچسب گذاری می‌کنیم. این سطح اطمینان برای هر نوع برنامه کاربردی مشابهی با استفاده از دارایی‌های اطلاعاتی C1, C2 یا C3 استفاده خواهد شد. منطق این نوع تصمیم‌گیری این است که هزینه اضافی استفاده از واپایش‌های امنیتی زیاد برای برنامه کاربردی C1 و C2 بیش از سود هنگفت حاصل از کارایی کاربرد مجدد سطح اطمینان موجود جبران می‌شود.

مثال ۴- همان سازمان فرایند مذکور را برای برنامه کاربردی با استفاده از اطلاعات C2 انجام می‌دهد و به‌عنوان خدمات اینترنتی پیشنهاد می‌کند. مجموعه ASCهای پیاده‌سازی شده برای این برنامه کاربردی به‌طور قابل ملاحظه‌ای (٪۵۰ از ASCهای جدید) نسبت به بانک ASC موجود اختلاف دارد. کارگروه ONF تصمیم می‌گیرد آن را به‌عنوان سطح جدید اطمینان در بانک وارد کرده و آن را به‌عنوان C2 برنامه کاربردی در معرض اینترنت برچسب بزند. به علت اینکه ٪۵۰ از ASCها مجددا استفاده می‌شوند، سازمان از مزیت سود حاصل از کارایی برخوردار است.

مثال ۵- همان سازمان فرایندی را برای برنامه کاربردی جدید انجام می‌دهد که مشابه با مورد مطرح در مثال ۲ است به استثنای اینکه عمدتا از دارایی‌های C4 استفاده می‌کند که برای این سازمان بحرانی در نظر گرفته می‌شوند و خصوصا منوط به الزامات قانونی و امنیتی هستند. مجموعه ASCهای پیاده‌سازی شده برای این برنامه کاربردی به‌طور قابل ملاحظه‌ای با هر سطح اطمینانی در بانک ASC تفاوت دارد: ٪۷۰ از ASCهای جدید، اکثرا مورد پایش قرار گرفته و واپایش‌های پاسخگو در مرحله کاربرد چرخه عمر سازمان هستند که کاملا برای پیاده‌سازی هزینه‌بر هستند. کارگروه ONF تصمیم به ورود آن به‌عنوان سطح جدید کلی اعتماد در بانک ASC گرفته و آن را به‌عنوان «C4 برنامه کاربردی از نوع کارخواه-کارساز بدون قرار گرفتن در معرض اینترنت» برچسب می‌زند. این سطح اطمینان برای هر نوع برنامه کاربردی مشابهی با استفاده از دارایی‌های اطلاعاتی C4 استفاده خواهد شد ولی تنها به علت هزینه هنگفت عملیات برنامه کاربردی در این سطح امنیت عمل خواهد کرد. از آنجا که ٪۳۰ از ASCها مجددا استفاده می‌شوند، سازمان باز هم از مزیت سود کسب شده از کارایی برخوردار خواهد شد.

مثال ۶- سازمان به نحو داخلی برنامه کاربردی بحرانی را تحت عنوان «حفظ» توسعه داده است که موجب امنیت سازمان تا حدی می‌شود که می‌تواند به آن برسد. طی دوره پروژه برنامه کاربردی بحرانی جدید، مالک برنامه کاربردی اعلان می‌کند که تمایل به اعتماد به این برنامه کاربردی جدید به اندازه اعتماد به برنامه «حفظ» دارد. کارگروه ONF تصمیم می‌گیرد که فرایند فوق را در اولویتی نسبت به برنامه «حفظ» انجام دهد. سطح حاصله از این اعتماد «همانند حفظ» برچسب می‌خورد. کارگروه ONF فرایند فوق را برای برنامه کاربردی جدید انجام می‌دهد و تعیین می‌کند که الزامات امنیتی واقعا بیش از حد کفایت پوشش‌دهی توسط ASCها، در برنامه «همانند حفظ» در نظر گرفته شوند و مالک برنامه کاربردی این سطح اطمینان را به نحوی برآورده می‌کند که سطح اطمینان او، سطح اطمینان برنامه «همانند حفظ» باشد.

چنانکه در مثال‌های قبلی مشاهده شده و در استاندارد ملی ایران شماره ۱-۲۷۰۳۴ بیان می‌شود، سطح اطمینان به سادگی برچسب در نظر گرفته شده برای مجموعه‌ای از ASCها در پاسخ به الزامات امنیتی یک یا چند برنامه کاربردی است و بنابراین سطحی که سازمان می‌تواند به برنامه کاربردی اطمینان کند، برچسب

موردنظر است. هیچ نوع علامت‌گذاری برای آن تعیین نشده است و الزامی برای رعایت ترتیب در میان سطوح اطمینان وجود ندارد.

یادآوری ۱- استاندارد ملی ایران شماره ۱-۲۷۰۳۴، شکل ۵ سطح اطمینان برچسب خورده از صفر الی ۵ را نشان می‌دهد، با این وجود این مورد صرفا مثالی در این زمینه است.

هنگام یکپارچگی واپایش‌ها از سوی طرف سوم، توصیه می‌شود سازمان نگاشتی از اطلاعات خاص طرف سوم به اطلاعات خودش داشته باشد.

مثال ۷- به تبعیت از توصیه گروه توسعه ASC، سازمانی تصمیم می‌گیرد ASCها را از فروشنده ASC طرف سوم به منظور پیاده‌سازی انواع مختلف آزمون امنیت برای برنامه‌های کاربردی خود خریداری کند. به‌طور طبیعی، ASCهای خریداری شده، برای بانک مختلف ASC طراحی شده و سطوح اطمینان توصیه شده آنها با سازمان انطباق نمی‌یابد. خوشبختانه ASCهای خریداری شده به زبان تبادل قابل حمل و بازی برای ASCهای توصیه شده در استاندارد ISO/IEC 27034-5 صادر شدند که محدوده فروشندگانی از سطوح اطمینان طبق تعریف ASCها را شامل می‌شود. سازمان این محدوده را با محدوده خودش مقایسه کرده و نگاشت ساده‌ای را ایجاد می‌کند که امکان یکپارچگیASCها در بانک ASC را فراهم می‌آورد.

یادآوری ۲- استاندارد ISO/IEC 27034-5 مورد مطالعه مفصلی را برای یکپارچگیASCهای طرف سوم فراهم می‌آورد.

مثال ۸- پیوست ب توصیف خلاصه‌ای از پروژه واقعی را برای پیاده‌سازی ONF در سازمان بزرگی فراهم می‌آورد. جریان کاری مورد استفاده برای این پروژه، مخصوص سازمان بوده و توسط گروه پروژه طراحی می‌شود. این مورد به‌عنوان مثالی نشان داده شده و به‌عنوان فرایند مورد نیاز برای پیاده‌سازی ONF در هر سازمانی محسوب نمی‌شود.

۸-۵-۵ واپایش امنیتی برنامه کاربردی

۱-۸-۵-۵ مقصود

این مولفه واپایش امنیت را برای تسهیل تایید، حفظ، کاربرد، درستی‌سنجی و ابلاغ آن، مستندسازی می‌کند.

۲-۸-۵-۵ مندرجات

استاندارد ملی ایران شماره ۱-۲۷۰۳۴ بازنگری مولفه واپایش امنیت برنامه کاربردی ASC و توصیفی از داده‌ها را فراهم می‌آورد که ASC را تشکیل می‌دهند. سازمان‌ها می‌توانند ASCها را با استفاده از رویکرد روایتی یا سفارشی پیاده‌سازی کنند که شامل کمینه توصیه‌های شناسایی شده در استاندارد ملی ایران شماره ۱-۲۷۰۳۴ زیربند ۵-۶-۲-۱-۸ می‌شود.

۳-۸-۵-۵ راهنما

واپایش‌های امنیت کاربردی در بانک مربوط گنجانده می‌شوند.

توصیه می‌شود ASC برای توصیف رسمی هر فعالیت امنیتی که سازمان تمایل به انجام آن در هر مرحله‌ای از چرخه عمر برنامه کاربردی خود دارد، ایجاد شود.

دیگر مولفه‌های ONF توصیف شده در این استاندارد، مجموعه‌هایی از مقادیر مجاز را به تبعیت از خصوصیت‌های ذکر شده در زیربندهای ۸-۱-۲-۶-۵-۳ و ۸-۱-۲-۶-۵-۴ از استاندارد ملی ایران شماره ۱-۲۷۰۳۴و زیربند ۵-۲ از استاندارد ISO/IEC 27034-5 تامین می‌کنند:

الف- الزامات عنوان شده (به زیربندهای ۵-۵-۲-۳ و ۵-۵-۳-۳ و ۵-۵-۵-۳ مراجعه شود)؛

ب- نقش‌ها، مسئولیت‌ها و صلاحیت‌های مورد نیاز (به زیربند ۵-۵-۶-۳ مراجعه شود) و

پ- چه زمانی (به زیربند ۵-۵-۹-۳ مراجعه شود).

استانداردهای ISO/IEC 27034-5 و ISO/IEC 27034-5-1 ساختار تفصیلی‌تر و انواعی را برای همه مولفه‌های داده ASC فراهم می‌آورد. سازمان‌ها ممکن است از این امکان برای ایجاد ASCهایی با قابلیت تعامل‌پذیری بهره‌مند شوند که می‌توانند با دیگر سازمان‌ها ابلاغ شوند.

همچنین، این ساختار، فیلد داده‌هایی را فراهم می‌آورد که به سازمان‌ها برای ارجاع متقابل به اطلاعات ASC کمک می‌کند و آن را برای فرایندهای سازمان مانند مدیریت تغییر، مدیریت سازگاری و مدیریت مخاطره قابل دسترس می‌کند.

استاندارد ISO/IEC 27034-6 مثال‌هایی از ASCهای ایجاد شده با استفاده از ساختار داده‌ها را فراهم می‌آورد.

در مورد نقش‌های در ارتباط با فعالیت‌های امنیتی و اندازه‌گیری درستی‌سنجی ASCها، توصیه می‌شود به وضوح همراه با نقش‌های دیگر در چرخه عمر برنامه کاربردی سازمان تعریف و مستندسازی شوند. توصیه می‌شود که مسئولیت‌های واضحی به‌عنوان مثال با استفاده از نمودارهای RACI تخصیص یابند.

توصیه می‌شود شواهد، تضمینی را فراهم آورند مبنی بر اینکه نقش‌ها در ارتباط با فعالیت‌های امنیتی و اندازه‌گیری‌های درستی‌سنجی دارای صلاحیت‌های مورد نیاز هستند. همانند هر مولفه ONF به سازمان توصیه می‌شود ASCهایی را از طریق فرایندهای مدیریت ONF توصیف‌شده طبق زیربندهای ۵-۴-۴، ۵-۴-۵، ۵-۴-۶ و ۵-۴-۷ ایجاد کرده، مرور کرده و بهبود بخشد.

در نتیجه فرایند طراحی ONF، توصیه می‌شود کارگروه ONF، ASCهایی را انتخاب کند که لازم است طی چرخه مدیریت ONF کنونی مطابق با اولویت‌های کنونی سازمان توسعه یابند. در مورد ASCها، چنین اولویت‌هایی اغلب توسط مخاطرات کنونی سازمان و نیازهای فوری در پروژه‌های برنامه کاربردی نشان داده می‌شوند.

سپس توصیه می‌شود کارگروه ONF، فرایند پیاده‌سازی ONF را انجام دهد. برای هر یک از ASCهای منتخب یا گروهی از ASCهای مرتبط، توصیه می‌شود:

الف- تخصیص گروه توسعه ASC، که ترکیب آن به بدنه دانش مورد نیاز به منظور دستیابی به راه‌حل کافی (یعنی فعالیت امنیتی و فعالیت درستی‌سنجی) برای الزامات امنیتی خاص ASC طبق سطوح اطمینان توصیه شده، وابسته است.

یادآوری- هنگام ایجاد، بازنگری یا بهبود ASC، به کارگروه ONF توصیه می‌شود منابع و تخصص‌های مورد نیاز بالأخص به شکل کارشناسان حوزه را برای دامنه خاصی که ASC از آن‌ها استفاده می‌کند، به‌دست آورد.

مثال: کارشناسان قانونی، کارشناسان پزشکی قانونی، کارشناسان فناوری، کارشناسان رمزنگاری، کارشناسان حریم خصوصی

ب- ابلاغ اهداف مدیریت و هدایت گروه توسعه که عمدتا از طریق الزامات امنیتی و سطوح اطمینان توصیه شده برای ASC صورت می‌گیرد؛

پ- تامین منابع کافی برای گروه توسعه، به شکل زمان، بودجه، مدیریت پروژه، ابزار، مستندسازی، آموزش و منابع فنی مانند آزمایشگاه‌های توسعه؛

ت- فراهم آوردن امکان طراحی، توسعه و پیاده‌سازی ASC برای گروه توسعه که معمولا توصیه می‌شود از آغاز تا انتهای فعالیت‌های پروژه انجام شود؛

ث- اعتبار بخشی به طراحی، تایید ASC به تازگی توسعه‌یافته و گنجاندن آن در بانک ASC؛

ج- تامین آموزش کافی برای بازیگران، طبق آنچه که توسط گروه توسعه مطابق با نقش‌ها، مسئولیت‌ها و صلاحیت‌های مورد نیاز برای فعالیت امنیتی و درستی‌سنجی ASC تعیین شده است.

طی دوره توسعه و پیاده‌سازی ASC، توصیه می‌شود گروه توسعه راه‌حل کافی را برای الزامات امنیتی و سطوح اطمینان توصیه شده از سوی کارگروه ONF تامین کند. به گروه توصیه می‌شود:

الف- کسب درک کاملی از الزامات امنیت ابلاغ شده از سوی کارگروه ONF، تاریخ و محتوای آن. این مورد اغلب در ارتباط با برگزاری جلساتی با نهادها و اشخاص سازمان در منشأ نیاز مانند گروه پروژه برنامه کاربردی یا خواندن الزامات مستندسازی شده از پروژه برنامه کاربردی است. درک معنی سطوح اطمینان توصیه شده برای ASC اساسی محسوب می‌شود. این اطلاعات از بانک ASC حاصل می‌شود.

ب- ایجاد مخزنی از راه‌حل‌های موجود. ممکن است در ارتباط با جستجوی بانک ASC برای ASCهایی برای رفع همان الزام امنیتی یا مشابه آن، جستجو برای ASCهای موجود در خارج از سازمان یا جستجوی واپایش‌های موجود باشد که تاکنون در ساختار داده‌ای ASC توصیف نشده‌اند.

پ- کسب درک کافی از زمینه قانونی، کسب‌وکار و فناوری موجود که در مورد الزامات امنیتی به منظور حذف راه‌حل‌هایی به کار می‌رود که مطابق با زمینه سازمان نبوده یا به سادگی با آن یکپارچه نمی‌شود.

ت- آزمون راه‌حل‌های مختلف و انتخاب بهترین راه‌حلی که مخاطره امنیتی شناخته شده در الزامات امنیتی را در زمینه سازمان کمینه کند.

ث- کسب درک کاملی از راهنما و اصول راهنمایی برای ASC در حال توسعه. توصیه می‌شود این اطلاعات توسط مولفه‌های ONF تامین شود. به‌عنوان مثال:

مثال ۱- راهنمای ASC و اصول راهنمای مربوط به خصوصیات ASC، دامنه‌های مقادیر، قواعد، علامت‌گذاری‌ها و وابستگی‌هایی را برای هر خصوصیت تامین می‌کند.

مثال ۲- محتواهای کسب‌وکار، مقرراتی و فناوری الزاماتی را برای ارجاع به خصوصیت نیازهای تعیین شده ASC تامین می‌کند.

مثال ۳- نقش‌ها، مسئولیت‌ها و مخزن صلاحیت، مقادیری را برای نقش‌ها و مسئولیت‌ها در توصیف فعالیت‌های امنیت و درستی‌سنجی ASC تامین می‌کند.

مثال ۴- مدل مرجع چرخه عمر امنیت برنامه کاربردی مقادیری را برای خصوصیت «چه موقع» در توصیف فعالیت‌های امنیتی و درستی‌سنجی ASC تامین می‌کند.

ج- مستندسازی راه‌حل به شکل ASC از طریق تامین مقادیری برای هر ASC مطابق با راهنما و اصول راهنمای سازمان.

ASC جدید ممکن است یکی از موارد زیر باشد:

الف- ASC کاملاً جدید یا

ب- دوباره‌کاری ASC موجود برای الزامات مختلف.

۱- نمونه جدید ASC موجود برای الزامات مختلف.

۲- نمونه‌سازی دقیق‌تر ASC والد[1].

۳- نسخه جدید ASC موجود، با زمینه تقویت یا تصحیح شده.

توصیه می‌شود ASC جدید به حد کافی در بانک ASC به منظور تسهیل کاربرد مجدد قرار داده شود. یعنی توصیه می‌شود از طریق خصوصیت والدها به ASCهای والد کافی پیوند بخورد. علاوه بر این ASC جدید ممکن است به بانک به‌عنوان والدی نسبت به ASCهای دیگر وارد شود که توصیه می‌شود برای انعکاس این‌گونه خصوصیت، والد بودن تغییر یابد.

یادآوری- به سازمان توصیه می‌شود هر اندازه بانک پیچیده‌تر شود، کاربرد راه‌حل فناوری برای مدیریت آن در نظر گرفته شود.

در برخی موارد، خصوصا هنگامی که سازمان در مراحل اولیه پیاده‌سازی ONF است، کارگروه توسعه اکثرا سازگار با رونویسی واپایش‌های موجود در ساختار داده ASC خواهد بود. به ترتیبی این‌گونه ساختار داده امکان افزودن پیوندهایی به طراحی کنترل مستندسازی شده موجود یا حتی پیوست چنین اسنادی به ASC را فراهم می‌آورد.

1 - Parent

هر چقدر سازمان‌ها از واپایش‌های موجود در الگوهای ASC بیشتر رونویسی کنند و آن‌ها را در دسترس قرار دهند، توسعه گروه‌ها برای کسب ASCها از دیگر سازمان‌ها و تطابق آن‌ها با الزامات و محتواهای سازمان ساده‌تر خواهد شد. در چنین مواردی، پیشنهاد می‌شود نسخه‌های جدید ASC نسبت به ASCهای کسب‌شده برای حفظ نسخه‌های اصلی برای اهداف مرجع تطبیق یابند.

توصیه می‌شود هر ASC تکمیل شود یعنی توصیه می‌شود گروه توسعه مقداری را برای هر خصوصیت در الگو فراهم کند، حتی اگر مقدار ناقص یا نامعلوم باشد. این روند اطلاعات بیشتری را نسبت به خصوصیت خالی فراهم می‌آورد زیرا نشان می‌دهد که خصوصیت واقعا در نظر گرفته شده و تصمیم‌گیری انجام شده است، حتی اگر تصمیم این بود که مقدار هنوز نامعلوم است.

۵-۵-۹ مدل مرجع چرخه عمر امنیت برنامه کاربردی

۵-۵-۹-۱ مقصود

مقصود از این مولفه این است که:

الف- به سازمان در ارائه زمان کاربرد ASC در چرخه عمر برنامه کاربردی کمک کند (یعنی مجموعه‌ای از مقادیر مجاز را برای خصوصیت «چه موقع» ASC تامین کند).

ب- مرجعی برای نقش‌های مستلزم انجام فعالیت‌ها یا وظایف ASC تامین کند.

پ- به سازمان برای اعتباربخشی به هر یک از چرخه‌های عمر برنامه کاربردی از طریق تشخیص همه فعالیت‌ها و بازیگران کمک کند که به نحو بالقوه‌ای در ارتباط با امنیت برنامه کاربردی است.

ت- به سازمان برای تضمین این مورد کمک می‌کند که نگرانی‌های امنیتی به طرز صحیحی در همه مراحل چرخه‌های عمر برنامه کاربردی برطرف شوند.

ث- به سازمان برای کمینه کردن هزینه و تأثیر معرفی شیوه‌های استاندارد ISO/IEC 27034 در پروژه‌های برنامه کاربردی از طریق حفظ چرخه‌های عمر برنامه کاربردی موجود کمک می‌کند.

ج- ارتباط بین گروه‌های در ارتباط با دامنه‌های مختلف دانش را تسهیل می‌کند.

چ- سازمان با مدل استاندارد را برای همسویی ASCها بین گروه‌های پروژه برنامه کاربردی، با وجود تفاوت در چرخه‌های عمر برنامه کاربردی، فراهم می‌آورد و

ح- سازمان‌ها با مدل استاندارد را برای به اشتراک گذاری ASCها با دیگر سازمان‌ها، با وجود تفاوت در چرخه‌های عمر برنامه کاربردی، تامین می‌کند.

۵-۵-۹-۲ توصیف

این مولفه، مدل چرخه عمر امنیت برنامه کاربردی مرجع را فراهم می‌آورد که با مدل‌های سازمانی مربوط تطبیق می‌یابد. فهرست استانداردی از حیطه‌های فعالیت، فعالیت‌ها و نقش‌های در ارتباط با مدیریت، مهندسی نرم‌افزار، زیرساخت فناوری اطلاعات و ممیزی برنامه کاربردی به‌عنوان مدل مرجعی برای چرخه عمر برنامه کاربردی در نظر گرفته می‌شود و به سازمان برای شناخت و ابلاغ یکنواخت هنگام حضور در چرخه عمر برنامه کاربردی و توصیه این مورد که ASCها توسط چه کسی پیاده‌سازی شود، کمک می‌کند.

طبق توصیف شکل ۳، این مدل مرجع به لحاظ افقی به دو مرحله عمده تقسیم می‌شود: ارائه مجوز و عملیات می‌تواند باز هم به موارد زیر تقسیم شود:

الف- مراحل ارائه مجوز از سه مرحله تشکیل می‌شود: آماده‌سازی، شناخت و انتقال.

ب- مراحل عملیات از سه مرحله تشکیل می‌شود: کاربرد و نگهداری، بایگانی و تخریب.

این مدل مرجع به لحاظ عمودی به چهار لایه تقسیم می‌شود:

الف- مدیریت برنامه کاربردی: این لایه از فعالیت‌های مربوط به دامنه حاکمیت مانند مدیریت پروژه و مدیریت عملیات برنامه کاربردی تشکیل می‌شود. چنین فعالیت‌هایی معمولا در فرایندهای تعریف شده در سامانه مدیریت امنیت اطلاعات سازمان انجام می‌شود.

ب- ارائه مجوز و عملیات برنامه کاربردی: این لایه از فعالیت‌های مربوط به ارائه مجوز و استفاده از برنامه کاربردی تشکیل می‌شود. چنین فعالیت‌هایی معمولا در فرایندهای قابل توصیه بر اساس استانداردهایی مانند استاندارد ISO/IEC 15026[۱] (همه قسمت‌ها)، استاندارد ISO/IEC 15288[۲]، استاندارد ISO/IEC 12207[۳] و استاندارد ISO/IEC 21827[۴] انجام می‌شوند.

پ- مدیریت زیرساخت: این لایه از فعالیت‌های مربوط به زیرساخت مدیریت خدمات فناوری اطلاعات سازمان برای حمایت از برنامه کاربردی تشکیل می‌شود. چنین فعالیت‌هایی معمولا در فرایندهای قابل توصیه طبق استانداردهایی مانند استاندارد ISO/IEC/ TR 20000-4 و محصولات راهنما مانند ITIL انجام می‌شوند و

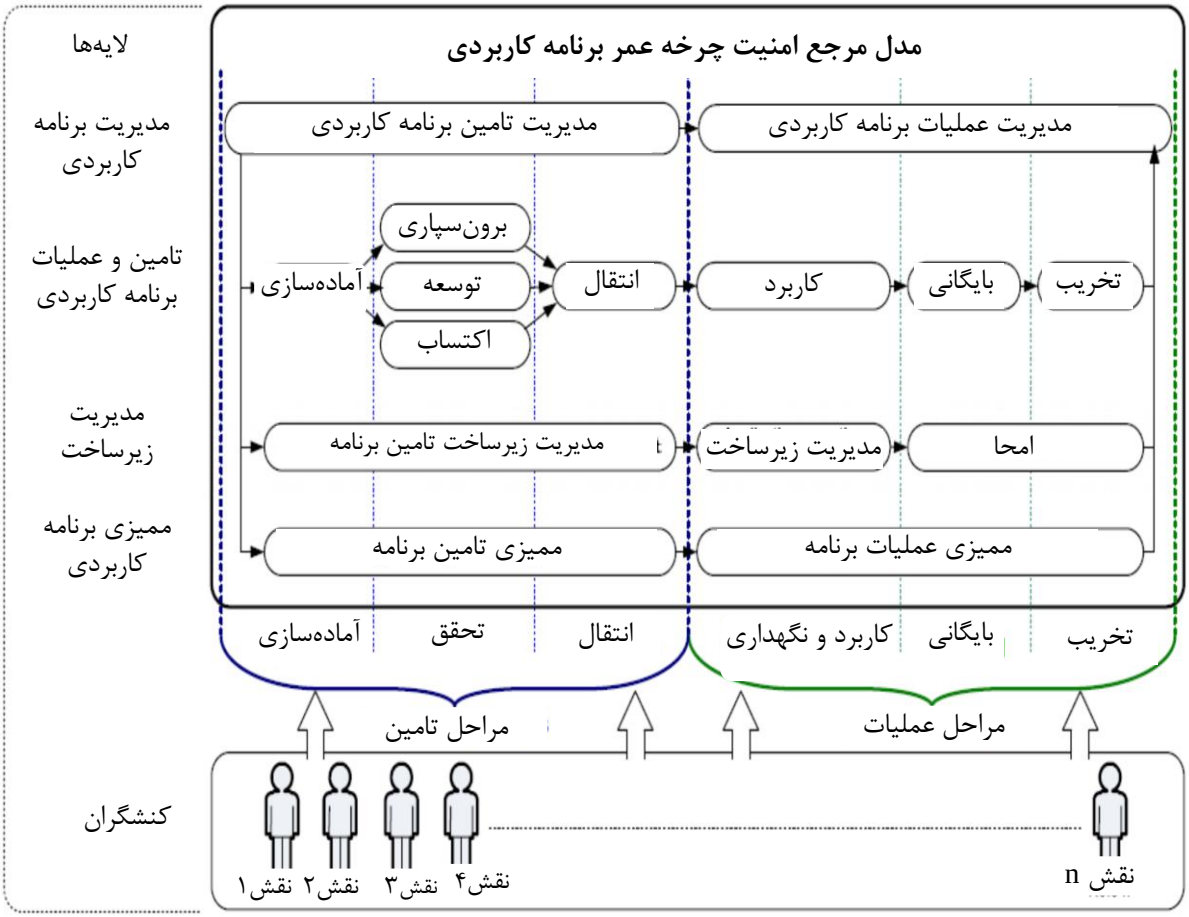
ت- ممیزی برنامه کاربردی: این لایه از فعالیت‌های مربوط به واپایش و درستی‌سنجی تشکیل می‌شود. چنین فعالیت‌هایی معمولا در فرایندهای قابل توصیه طبق استانداردهایی مانند استاندارد ISO/IEC 15288، استاندارد ISO/IEC 12207 و مستندات شیوه صنعتی مانند COBIT انجام می‌شود.

۱- استانداردهای ملی به شماره ۱۶۳۴۳ موجود است.

۲ - استاندار ملی به شماره ۱۶۳۰۴ مربوط به سال ۲۰۰۸ موجود است.

۳ - استاندارد ملی به شماره ۱۲۲۰۷ موجود است.

۴ - استانداردهای ملی به شماره ۲۱۸۲۷ مربوط به سال ۲۰۰۸ موجود است.



شکل ۳- نمایش نگاشتاری مدل مرجع چرخه عمر امنیت برنامه کاربردی

۵-۵-۹-۳ مندرجات

۵-۵-۹-۳-۱ نقش‌ها

توصیه می‌شود مدل مرجع چرخه عمر امنیت برنامه کاربردی، فهرستی از نقش‌ها را برای همه بازیگران در ارتباط با فعالیت‌های مدل مرجع چرخه عمر امنیت برنامه کاربردی فراهم آورده و به سازمان برای شناسایی و ابلاغ یکنواخت نقش‌ها، مسئولیت‌ها و صلاحیت‌های مورد نیاز به واسطه تامین مجموعه‌ای از مقادیر مجاز برای خصوصیت «نقش‌ها، مسئولیت‌ها و صلاحیت‌های مورد نیاز» ASCها کمک کند.

برای این مجموعه مقادیر مجاز، اکیدا توصیه می‌شود سازمان از فهرست استانداردی از نقش‌های تامین شده در استاندارد ISO/IEC 27034-5 استفاده کند. این روند، به اشتراک‌گذاری ASCها با گروه‌های پروژه‌ای مختلف در سازمان یا همراه با سازمان‌های مختلف را فراهم می‌آورد.

۵-۵-۹-۳-۲ فعالیت‌ها

توصیه می‌شود مدل مرجع چرخه عمر امنیت برنامه کاربردی فهرست تفصیلی از فعالیت‌ها به‌عنوان مجموعه‌ای از مقادیر مجاز را برای خصیصه «چه موقع» ASC تامین کند. به سازمان توصیه می‌شود از فهرست استاندارد فعالیت‌های تامین شده طبق استاندارد ISO/IEC 27034-5-1 استفاده کند. این روند، به اشتراک‌گذاری ASCها با گروه‌های پروژه‌ای مختلف در سازمان یا همراه با سازمان‌های مختلف را فراهم می‌آورد.

فعالیت‌ها معمولا در مراحل مدل مرجع چرخه عمر امنیت برنامه کاربردی انجام شده و طبق شکل ۳ به شرح زیر توصیف می‌شوند.

۵-۵-۹-۳-۲-۱ مدیریت در ارائه مجوز برنامه کاربردی

فعالیت‌های مدیریت ارائه مجوز برنامه کاربردی توسط مدیران پروژه‌ای و سازمانی طی مراحل ارائه مجوز چرخه عمر برنامه کاربردی انجام می‌شوند.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای در سطح وسیع سازمانی انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار از گروه فرایندهای پروژه‌ای تعریف شده طبق استاندارد ISO/IEC 12207، مانند فرایند مدیریت منابع انسانی، فرایند طرح‌ریزی پروژه، ارزیابی پروژه و فرایند واپایش و فرایند مدیریت تصمیم‌گیری می‌شود.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند آغاز، طرح‌ریزی، اجرا، پایش و واپایش و بستن تقسیم کند.

۵-۵-۹-۳-۲-۲ مدیریت عملیات برنامه کاربردی

فعالیت‌های مدیریت عملیات برنامه کاربردی مربوط به مدیریت و استفاده از برنامه کاربردی طی مراحل عملیات است.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای در سطح وسیع سازمان انجام می‌گیرند. این فعالیت‌ها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند مدیریت تصمیم‌گیری و فرایند مدیریت اطلاعات می‌شود.

معمولا برنامه کاربردی تحت مسئولیت مالک آن ممکن است به اشتراک‌گذاری برخی از مسئولیت‌ها با دیگر بازیگران مانند مدیران کاربر را برگزینند.

توصیه می‌شود تغییرات نسبت به برنامه کاربردی طی مراحل عملیات، مانند تغییرات ناشی از الزامات مقرراتی جدید یا تهدیدات، توسط مالک برنامه کاربردی که مسئول تضمین این موضوع است که برنامه کاربردی به درستی و به نحو پیوسته‌ای نیازهای امنیتی در حال تغییر سازمان را برطرف می‌کند، آغاز شوند.

از طریق این فرایندها، مالک برنامه کاربردی، سامانه مدیریت امنیت اطلاعات را با شواهد و تضمین مورد نیاز تامین خواهد کرد تا پروژه‌های حاکمیت برنامه کاربردی تعیین شوند.

به منظور تعیین دقیق‌تر مشخصات اینکه بهتر است چه موقع فعالیت‌های امنیتی انجام شوند، سازمان مجاز است باز هم این ناحیه از فعالیت را به نواحی فرعی مانند آغاز، طرح‌ریزی، اجرا، پایش و واپایش و بستن تقسیم کند.

۵-۵-۹-۳-۲-۳ آماده سازی

طی مرحله آماده‌سازی، گروه ارائه مجوز فعالیت‌های مقدماتی یا آماده‌سازی را انجام می‌دهد. چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایند وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207 مانند زیربند ۶-۳-۳ فرایند مدیریت تصمیم‌گیری و زیربند ۶-۳-۶ فرایند مدیریت اطلاعات می‌شود.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند آغاز و طرح‌ریزی تقسیم کند.

۵-۵-۹-۳-۲-۴ برون‌سپاری

طی مرحله شناخت، فعالیت‌های مربوط به پیاده‌سازی نرم‌افزار از طریق گروه ارائه مجوز انجام می‌شوند. در صورتی که سازمان برخی فعالیت‌های پیاده‌سازی را به صورت برون‌سپاری انجام دهد، ممکن است به افزودن ASCهای خاص برای پیاده‌سازی فعالیت‌ها به منظور کسب سطح اطمینان برنامه کاربردی هدف نیاز دارد. به همین دلیل، مدل مرجع چرخه عمر امنیت برنامه کاربردی حیطه فعالیت خاصی را برای برون‌سپاری ارائه می‌دهد.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند اکتساب، فرایند مدیریت مستندسازی نرم‌افزار، فرایند مدیریت پیکربندی نرم‌افزار و فرایند مدیریت مخاطره می‌شود.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند شناخت و گذار تقسیم کند.

۵-۵-۹-۳-۲-۵ توسعه

فعالیت‌های مربوط به پیاده‌سازی نرم‌افزار توسط گروه ارائه مجوز طی مرحله شناخت انجام می‌شوند. در صورتی‌که سازمان در حال انجام برخی از فعالیت‌های پیاده‌سازی به شیوه داخلی است، ASCها به فعالیت‌های پیاده‌سازی اضافه می‌شوند که ممکن است از با ASCهای اضافه شده هنگام خرید یا برون‌سپاری مولفه پیاده‌سازی یا برنامه کاربردی متفاوت باشند. به همین دلیل، مدل مرجع چرخه عمر امنیت برنامه

کاربردی، حیطه خاصی را برای توسعه فعالیت‌هایی ارائه می‌دهد که منجر به پیاده‌سازی توسعه داخلی نرم‌افزار می‌شود.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند مدیریت مخاطره، فرایند طراحی معماری نرم‌افزار، فرایند طراحی تفصیلی نرم‌افزار، فرایند ساخت نرم‌افزار، فرایند مدیریت مستندسازی نرم‌افزار، فرایند مدیریت پیکربندی نرم‌افزار، فرایند درستی‌سنجی نرم‌افزار، فرایند اعتبارسنجی نرم‌افزار، فرایند مرور کلی نرم‌افزار، فرایند مهندسی دامنه و فرایند مدیریت دارایی با قابلیت استفاده مجدد می‌شوند.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند آغاز، بیان دقیق، ساخت و پیاده‌سازی تقسیم کند.

۵-۵-۹-۳-۲-۶ اکتساب

فعالیت‌های اکتساب ممکن است از طریق گروه ارائه مجوز به هدف اکتساب یا خرید محصول یا خدماتی به شیوه داخلی انجام شود که نیازهای سازمان را برآورده کند. ASCهای خاص ممکن است به فعالیت‌ها اضافه شود. از این رو، مدل مرجع چرخه عمر امنیت برنامه کاربردی، حیطه خاصی را برای فعالیت‌های اکتسابی نشان می‌دهد که منجر به پیاده‌سازی مولفه‌های برنامه کاربردی مورد نیاز می‌شود.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این موارد شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند اکتساب، فرایند مدیریت مستندسازی نرم‌افزار، فرایند مدیریت پیکربندی نرم‌افزار، فرایند مدیریت مخاطره و فرایند پیاده‌سازی می‌شوند.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند طرح‌ریزی و بستن تقسیم کند.

۵-۵-۹-۳-۲-۷ انتقال

این حیطه در مرحله انتقال شامل فعالیت‌هایی می‌شود که توسط گروه ارائه مجوز برای آماده‌سازی، پیکربندی، آزمون و استقرار برنامه کاربردی در محیط عملیاتی تعریف شده از سوی سازمان انجام می‌پذیرند.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند مدیریت پیکربندی نرم‌افزار، فرایند یکپارچگی سامانه و فرایند آزمون صلاحیت سامانه است.

۵-۵-۹-۳-۲-۸ کاربرد

فعالیت‌هایی که طی کاربرد و مرحله نگهداری انجام می‌شوند در ارتباط با کاربرد برنامه کاربردی در محیط عملیاتی توسط همه کاربران هستند. چنین فعالیت‌هایی شامل کاربر و مدیریت دسترسی، ثبت، پایش، آموزش امنیت و مواردی از این قبیل هستند.

دیگر فعالیت‌ها برای نگهداری نرم‌افزار و مدیریت تغییر انجام می‌پذیرند که شامل به‌روزرسانی نرم‌افزار برنامه کاربردی به منظور تغییر الزامات اطلاعاتی مانند افزودن توابع جدید و تغییر فرمت‌های داده می‌شوند. این رویه شامل رفع اشکالات و تطابق نرم‌افزار با وسایل سخت‌افزاری جدید می‌شود.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند عملیات نرم‌افزار و فرایند نگهداری نرم‌افزار است.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند کاربرد و نگهداری تقسیم کند.

۵-۵-۹-۳-۲-۹ بایگانی

فعالیت‌های مربوط به بایگانی توسط گروه عملیات هنگامی انجام می‌شوند که برنامه کاربردی، دیگر به وضعیت فعال نیاز ندارد. این‌گونه فعالیت‌ها شامل بایگانی همه اطلاعات برنامه کاربردی از جمله بایگانی همه ابزار و فرایندها برای حفظ و دستیابی امن به این نوع اطلاعات هستند، حتی در صورتی که برنامه کاربردی در حال اجرا در محیط عملیاتی نیست.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند امحا نرم‌افزار می‌شود.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند طرح‌ریزی، انجام و درستی‌سنجی تقسیم کند.

۵-۵-۹-۳-۲-۱۰ تخریب

فعالیت‌های تخریبی در ارتباط با تخریب امنیت همه اطلاعات امنیتی است که شامل داده‌های کاربری، اطلاعات سازمان، ثبت‌های کاربر، پارامترهای برنامه کاربردی و غیره می‌شود.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند امحا نرم‌افزار می‌شود.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند طرح‌ریزی، انجام و درستی‌سنجی تقسیم کند.

۵-۵-۹-۳-۲-۱۱ مدیریت زیرساخت ارائه مجوز برای برنامه کاربردی

فعالیت‌های مدیریت زیرساخت ارائه مجوز برنامه کاربردی در ارتباط با تامین و نگهداری زیرساخت فناورانه امن در حمایت از فعالیت‌های گروه ارائه مجوز هستند. این فعالیت‌ها شامل خدمات، تسهیلات، ابزار و ارتباطات و دارایی‌های فناوری اطلاعات در محیط توسعه و محیط‌های مختلف آزمون می‌شوند.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند مدیریت زیرساخت و فرایند مدیریت پیکربندی می‌شود.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند نصب، عملیات، نگهداری، حمایت و بایگانی تقسیم کند.

۵-۵-۹-۳-۲-۱۲ مدیریت زیرساخت عملیات برنامه کاربردی

فعالیت‌های مدیریت زیرساخت عملیات برنامه کاربردی، در ارتباط با تامین و نگهداری زیرساخت فناورانه امن برای مراحل عملیاتی چرخه عمر برنامه کاربردی هستند. این فعالیت‌ها شامل خدمات، تسهیلات، ابزار و ارتباطات و دارایی‌های فناوری اطلاعات در محیط عملیاتی برنامه کاربردی می‌شوند.

توصیه می‌شود دیگر فعالیت‌ها نیز طی مراحل عملیاتی برای نگهداری امنیتی زیرساخت در حمایت از برنامه کاربردی انجام شوند. نگهداری زیرساخت شامل نگهداری سامانه و سخت‌افزار شبکه، پشتیبان‌گیری و بازیابی، بازیابی فاجعه و غیره می‌شود.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند عملیاتی و فرایند نگهداری می‌شوند.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند حمایت، عملیات، نگهداری و بایگانی تقسیم کند.

۵-۵-۹-۳-۲-۱۳ امحا

فعالیت‌های امحا به منظور تضمین این موضوع انجام می‌شوند که همه اطلاعات ذخیره شده روی کارسازها، سامانه‌ها و دیگر اجزای فناوری مورد استفاده برنامه کاربردی به شیوه امنی حذف می‌شوند. این نوع تضمین

امکان امحا یا بازیابی این‌گونه اجزا را بدون ایجاد مخاطره امنیتی برای سازمان فراهم می‌آورد. چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 15288، مانند فرایند امحا می‌شوند.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند طرح‌ریزی، انجام و درستی‌سنجی تقسیم کند.

۵-۵-۹-۳-۲-۱۴ ممیزی ارائه مجوز برنامه کاربردی

فعالیت‌های ممیزی ممکن است نسبت به همه فعالیت‌ها، بازیگران، فرایندها، مصنوعات و مولفه‌های کاربردی مورد استفاده یا تولیدی طی چرخه عمر برنامه کاربردی انجام شوند.

این فعالیت‌ها ممکن است یک‌بار یا به‌طور متناوب توسط گروه‌های ممیزی داخلی یا خارجی بسته به سطح اطمینان پروژه برنامه کاربردی انجام شوند. آن‌ها مالک برنامه کاربردی را به همراه تضمین و شواهد مورد نیاز به نحوی تامین می‌کنند که الزامات امنیتی برای برنامه کاربردی طبق انتظار، برآورده شود.

فعالیت‌های ممیزی طی مراحل ارائه مجوز انجام می‌شوند که معمولا با فعالیت‌های انجام شده طی مراحل عملیات تفاوت دارند. سازمان‌های در حال توسعه برنامه‌های کاربردی ولی نه در حال عملیات (مانند خرده‌فروشان نرم‌افزار) ممکن است هرگز به ممیزی برنامه‌های کاربردی در مراحل عملیات نیاز نداشته باشند. از این رو، مدل مرجع چرخه عمر امنیت برنامه کاربردی، حیطه خاصی را برای ممیزی فعالیت‌های انجام شده طی مراحل ارائه مجوز ارائه می‌دهد.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایند وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند ممیزی نرم‌افزار هستند.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند طرح‌ریزی، اکتساب، پیاده‌سازی، تحویل، حمایت، پایش و ارزیابی تقسیم کند.

۵-۵-۹-۳-۲-۱۵ ممیزی عملیات برنامه کاربردی

فعالیت‌های ممیزی که طی مراحل عملیات انجام می‌شوند با فعالیت‌های ممیزی که طی مراحل ارائه مجوز انجام می‌پذیرند، تفاوت دارند. سازمان در حال عملیات تنها برنامه‌های کاربردی را کسب می‌کند که ممکن هرگز به ممیزی برنامه‌های کاربردی در مراحل ارائه مجوز نیاز نداشته باشند. از این رو، مدل مرجع چرخه عمر امنیت برنامه کاربردی، حیطه خاصی را برای فعالیت‌های ممیزیِ انجام‌شده طی مراحل عملیات ارائه می‌دهد.

چنین فعالیت‌هایی معمولا به‌عنوان قسمتی از فرایندهای وسیع در سطح سازمان انجام می‌شوند. این فرایندها شامل فرایندهای مهندسی نرم‌افزار طبق استاندارد ISO/IEC 12207، مانند فرایند ممیزی نرم‌افزار هستند.

به منظور مشخصات دقیق‌تر از اینکه چه موقع توصیه می‌شود فعالیت‌های امنیتی انجام شوند، ممکن است سازمان باز هم این حیطه از فعالیت را به حیطه‌های فرعی مانند طرح‌ریزی، اکتساب، پیاده‌سازی، تحویل، حمایت، پایش و ارزیابی تقسیم کند.

۵-۵-۱۰ مدل چرخه عمر امنیت برنامه کاربردی

۵-۵-۱۰-۱ مقصود

مقصود از این مولفه ONF عبارت است از:

الف- کمک به سازمان برای کشف و توصیف رسمی مدل‌های چرخه عمر امنیت برنامه کاربردی که تاکنون به کار گرفته شده‌اند؛

ب- کمک به سازمان برای تکمیل این‌گونه مدل‌ها در صورتی که به مدل مرجع چرخه عمر امنیت برنامه کاربردی توصیف شده در این استاندارد نیاز داشته باشند (یعنی افزودن لایه‌ها، مراحل، فعالیت‌ها یا بازیگران)؛

پ- تسهیل در برقراری ارتباط ASCها با گروه‌های توسعه برنامه کاربردی و

ت- تسهیل در یکپارچگی ASCها با دیگر فعالیت‌هایی که تاکنون توسط گروه‌های توسعه برنامه کاربردی انجام شده‌اند.

۵-۵-۱۰-۲ توصیف

مدل مرجع چرخه عمر امنیت برنامه کاربردی مبتنی بر مدل چرخه عمر برنامه کاربردی است ولی برای مدیریت فعالیت‌های امنیت برنامه کاربردی به کار گرفته می‌شود. توصیه می‌شود که این مدل لایه‌ها، مراحل و فعالیت‌ها را ارائه دهد.

۵-۵-۱۰-۳ مندرجات

توصیه می‌شود این جزء ONF نگاشتی از یک یا چند چرخه عمری را تامین کند که تاکنون به همراه مدل مرجع چرخه عمر امنیت برنامه کاربردی، در سازمان به کار گرفته شده‌اند.

۵-۵-۱۰-۴ راهنما

سازمان‌های مختلف از مدل‌های چرخه عمر متفاوتی استفاده می‌کنند. همچنین شیوه معمول در سازمان‌ها این است که مدل‌های چرخه عمر متفاوتی توسط گروه‌های توسعه مختلفی در قسمت‌های مختلف سازمان

در پروژه‌های متفاوتی استفاده شوند. این استاندارد به سازمان‌ها، تحمیل چرخه عمر استاندارد یا گروه‌های توسعه برنامه کاربردی را پیشنهاد نمی‌کند.

از این رو توصیه می‌شود ASCهایی که به فعالیت‌هایی از مدل مرجع چرخه عمر امنیت برنامه کاربردی(به بند ۵-۵-۹ مراجعه شود) استاندارد ارجاع می‌یابند، قبل از ابلاغ به گروه‌های برنامه کاربردی، به طریقی «ترجمه» شوند که با هر مدل چرخه عمر آشنای گروه و فعالیت‌ها یکپارچه شوند.

نگاشت ارائه شده توسط این جز به همین منظور به کار گرفته می‌شود که ممکن است به سادگی « ذکر جزئیات انواع» در جداول ارائه شده در استاندارد ISO/IEC 27034-5-1 همراه با ستون افزوده شده به ازای هر یک از مدل‌های چرخه عمر سازمان باشد. استاندارد ISO/IEC 27034-6 این روش را همراه با مطالعه موردی در مورد «کاربرد ASLCRM برای تسهیل پیاده‌سازی ASCها توسط گروه‌های مختلف توسعه در داخل سازمان» توصیف می‌کند.

توصیه می‌شود مراحل ارائه مجوز در مدل‌های چرخه عمر امنیت برنامه کاربردی شامل همه فعالیت‌های ارائه مجوز برنامه کاربردی سازمان شوند. توصیه می‌شود مراحل عملیات در مدل‌های چرخه عمر امنیت برنامه کاربردی سازمان شامل همه فعالیت‌های عملیاتی برنامه کاربردی سازمان شوند.

ممکن است افزودن لایه‌ها، مراحل، فعالیت‌ها یا بازیگران مورد نیاز به مدل چرخه عمر امنیت برنامه کاربردی به منظور اطمینان از این موضوع که هر ASC که به واسطه سطح اطمینان هدف برنامه کاربردی مورد نیاز است طی چرخه عمر برنامه کاربردی به حد کافی به‌کار برده شود.

نیاز به توسعه برنامه‌های کاربردی امن ممکن است بهبود مستمری را در مدل‌های چرخه عمر برنامه کاربردی سازمان بطلبد که توسط فرایند مدیریت ONF حمایت شده و مبتنی بر یافته‌های ممیزی قبلی و نتایج ارزیابی مخاطره به منظور تضمین این موضوع هستند که برنامه‌های کاربردی توسعه‌یافته مقاومت بهتری را نسبت به حملات ارائه داده و مخاطرات امنیتی غیرقابل قبولی را نشان نمی‌دهند.

توصیه می‌شود درحین بازنگری و بهبود مدل چرخه عمر امنیت برنامه کاربردی، کارگروه ONF و کارشناسان همکار حوزه از اهمیت تعریف، پیاده‌سازی، پایش و ابلاغ مدل چرخه عمر امنیت برنامه کاربردی مطابق با اهداف کسب‌وکار و امنیتی آن به واسطه اجزای الزامی سازمان، واپایش‌های امنیت برنامه کاربردی و فعالیت‌ها در کل چرخه عمر برنامه کاربردی آگاه باشند.

توصیه می‌شود درحین بازنگری و بهبود در مدل چرخه عمر امنیت برنامه کاربردی، ورودی‌های زیر در نظر گرفته شوند:

الف- مدل مرجع چرخه عمر امنیت برنامه کاربردی ارائه شده توسط این استاندارد (به زیربند ۵-۵-۹ مراجعه شود)؛

ب- چرخه‌های عمر برنامه کاربردی سازمان و فرایندهای چرخه عمر؛

پ- روش‌های توسعه نرم‌افزار سازمان؛

ت- واپایش‌های امنیت برنامه کاربردی سازمان؛

ث- نتایج ارزیابی مخاطره امنیت برنامه کاربردی؛

ج- بازخورد به‌دست آمده از توسعه‌دهندگان سازمان، مهندسین نرم‌افزار و کاربران در میان دیگر ذینفعان.

۵-۵-۱۱ فرایند مدیریت امنیت برنامه کاربردی

۵-۵-۱۱-۱ مقصود

فرایند مدیریت امنیت برنامه کاربردی امکان مدیریت امنیت برای هر برنامه کاربردی مورد استفاده را برای سازمان فراهم می‌آورد.

۵-۵-۱۱-۲ توصیف

فرایند مدیریت امنیت برنامه کاربردی، فرایند کلی برای مدیریت امنیت هر برنامه کاربردی مورد استفاده سازمان است. این فرایند، تخصصی از فرایند مدیریت مخاطره است که در استاندارد ISO/IEC 27005 ارائه شده است.

۵-۵-۱۱-۳ نتایج

در نتیجه انجام این فرایند، در رابطه با پروژه برنامه کاربردی نتایج زیر را خواهیم داشت:

الف- الزامات برنامه کاربردی و محیط تعیین می‌شود؛

ب- مخاطرات مربوط به امنیت اطلاعات برنامه کاربردی ارزیابی می‌شود؛

ج- الزامات امنیت برنامه کاربردی از ارزیابی مخاطره تعیین شده و به‌عنوان سطح اطمینان هدف برنامه کاربردی بیان می‌شوند؛

د- برخورد با مخاطره از طریق انتخاب ASCهای مناسب مطابق با سطح اطمینان هدف برنامه کاربردی آغاز می‌شود؛

ه- برخورد با مخاطرات امنیت اطلاعات برنامه کاربردی از طریق انجام فعالیت‌های امنیتی صورت می‌گیرد و اندازه‌گیری‌های درستی‌سنجی در ASCهای منتخب تعریف می‌شوند؛ و

و- مخاطره اضافی برنامه کاربردی از طریق تعیین سطح واقعی برنامه کاربردی در فرایند درستی‌سنجی امنیت برنامه کاربردی (زیربند ۵-۵-۱۳) اندازه‌گیری می‌شود.

۵-۵-۱۱-۴ فعالیت‌های تحقق

جدول ۱۵- نمودار RACI برای تحقق فرایند مدیریت امنیتی برنامه کاربردی

فعالیت‌های تحقق	مالک برنامه کاربردی	گروه توسعه برنامه کاربردی	ممیز
۱- انجام مرحله تشخیص الزامات و محیط برنامه کاربردی	A	R	
۲- انجام مرحله ارزیابی مخاطرات امنیتی برنامه کاربردی	A	R	
۳- انجام مرحله ایجاد و نگهداری چارچوب الزامی برنامه کاربردی		A/R	
۴- انجام مرحله تدارک و عملیات برنامه کاربردی		A/R	C
۵- انجام مرحله ممیزی امنیت برنامه کاربردی	A	C	R

۵-۵-۱۱-۵ فعالیت‌های درستی‌سنجی

جدول ۱۶- نمودار RACI برای درستی‌سنجی فرایند مدیریت امنیت برنامه کاربردی

فعالیت‌های درستی‌سنجی	کارگروه ONF	مالک برنامه کاربردی	گروه توسعه برنامه کاربردی	ممیز
۱- سنجش اینکه مرحله تشخیص الزامات برنامه کاربردی و محیط به درستی در دوره پروژه برنامه کاربردی سازمان انجام می‌شود.	A	C	C	R
۲- سنجش این موضوع که مرحله ارزیابی مخاطرات امنیت برنامه کاربردی به درستی در دوره پروژه برنامه کاربردی سازمان انجام می‌شود.	A	C	C	R
۳- سنجش این مورد که مرحله ایجاد و نگهداری چارچوب الزامی برنامه کاربردی به درستی در دوره پروژه برنامه کاربردی سازمان انجام می‌شود.	A		C	R
۴- سنجش این موضوع که مرحله تدارک و عملیات برنامه کاربردی به درستی در دوره پروژه برنامه کاربردی سازمان انجام می‌شود.	A		C	R
۵- سنجش این موضوع که مرحله ممیزی امنیت برنامه کاربردی در دوره پروژه برنامه کاربردی سازمان به درستی انجام می‌شود.		A	C	R

۵-۵-۱۱-۶ راهنما

مرور کلی ۵ مرحله ذکر شده در زیربند ۵-۵-۱۱-۴، در بندهای ۷ و ۸ استاندارد ISIRI 27034-1 ارائه می‌شود. توصیف تفصیلی فرایند مدیریت امنیت برنامه کاربردی موضوع استاندارد ISO/IEC 27034-3 بوده و راهنمای بیشتری در آن استاندارد بین‌المللی ارائه می‌شود.

ممیز مسئول هدایت فعالیت پنجم درستی‌سنجی طبق جدول ۱۶ است و توصیه می‌شود مستقل از ممیز فعالیت ۵ در جدول ۱۵ انجام شود. توصیه می‌شود استقلال ممیز نسبت به ممیزی‌شونده اثبات شود.

۵-۵-۱۲ فرایند تحلیل مخاطره امنیت برنامه کاربردی

۵-۵-۱۲-۱ مقصود

شناسایی و ارزشیابی مخاطرات امنیت برنامه کاربردی در کل چرخه عمر برنامه کاربردی برای تامین فرایند تحلیل مخاطره امنیت برنامه کاربردی قابل تکرار و ابزار تحلیل تایید توسط سازمان در نظر گرفته می‌شود.

۵-۵-۱۲-۲ توصیف

فرایند تحلیل مخاطره امنیت برنامه کاربردی، فرایندی برای درک مخاطره در مواجه هر برنامه کاربردی مورد استفاده سازمان است. این فرایند، تخصصی از قسمتی از فرایند مدیریت مخاطره است که در استاندارد ISO/IEC 27005 ارائه شده است.

۵-۵-۱۲-۳ مندرجات

این جز ONF، مستندسازی فرایندها، فعالیت‌ها و ابزار تایید شده توسط سازمان با هدف هدایت تحلیل مخاطره امنیت اطلاعات در حوزه و دامنه برنامه کاربردی محسوب می‌شود.

توصیه می‌شود جز ONF مواجه‌های امنیتی برنامه کاربردی مبتنی بر آسیب‌پذیری‌ها، تهدیدات و اثرات کسب‌وکار در ارتباط با دارایی‌های (اجزا) برنامه کاربردی و اولویت‌دهی به مخاطرات به وقوع پیوسته، شناسایی شوند.

۵-۵-۱۲-۴ راهنما

توصیه می‌شود سازمان فرایند تحلیل مخاطره امنیت برنامه کاربردی را تعریف یا انتخاب کند که برای تحلیل مخاطرات امنیت برنامه کاربردی کافی باشد. این مورد لزوما موردی برای همه فرایندهای تحلیل مخاطره محسوب نمی‌شود که اکثر آن‌ها برای مخاطره سازمانی طراحی نشده‌اند و ممکن است به سادگی کاهش نیابند.

توصیه می‌شود این فرایند قادر به هدایت در تشخیص مواجهه امنیت برنامه کاربردی مبتنی بر حوزه و دامنه ایجاد شده و در نظر گرفتن دارایی‌های (اجزا) در ارتباط با برنامه کاربردی باشد. توصیه می‌شود فرایند بر

دانش محیط عملیاتی تمرکز کند که برنامه کاربردی به کار می‌رود تا شناسایی کند که کدام جزء از برنامه کاربردی نسبت به تهدیدات خاص و پیامدهایی آسیب‌پذیر هستند که محرمانگی، یکپارچگی و قابلیت دسترسی که ممکن است برای اجزا مطرح باشند را از بین می‌برند. توصیه می‌شود فرایند تحلیل مخاطره امنیت برنامه کاربردی در حالی استفاده شود که مرحله ۲ یعنی ارزیابی مخاطرات امنیت برنامه کاربردی ASMP که در استاندارد ISIRI 27034-1، زیربند ۸-۳-۳ توصیف می‌شود، استفاده شود. بنابراین توصیه می‌شود از ورودی اطلاعات دانش به‌عنوان خروجی به‌دست آمده از مرحله ۱ تشخیص الزامات برنامه کاربردی و محیط ASMP استفاده شود مانند:

الف- کسب‌وکار برنامه کاربردی، محتواهای فناوری و مقرراتی و

ب- مشخصات برنامه کاربردی.

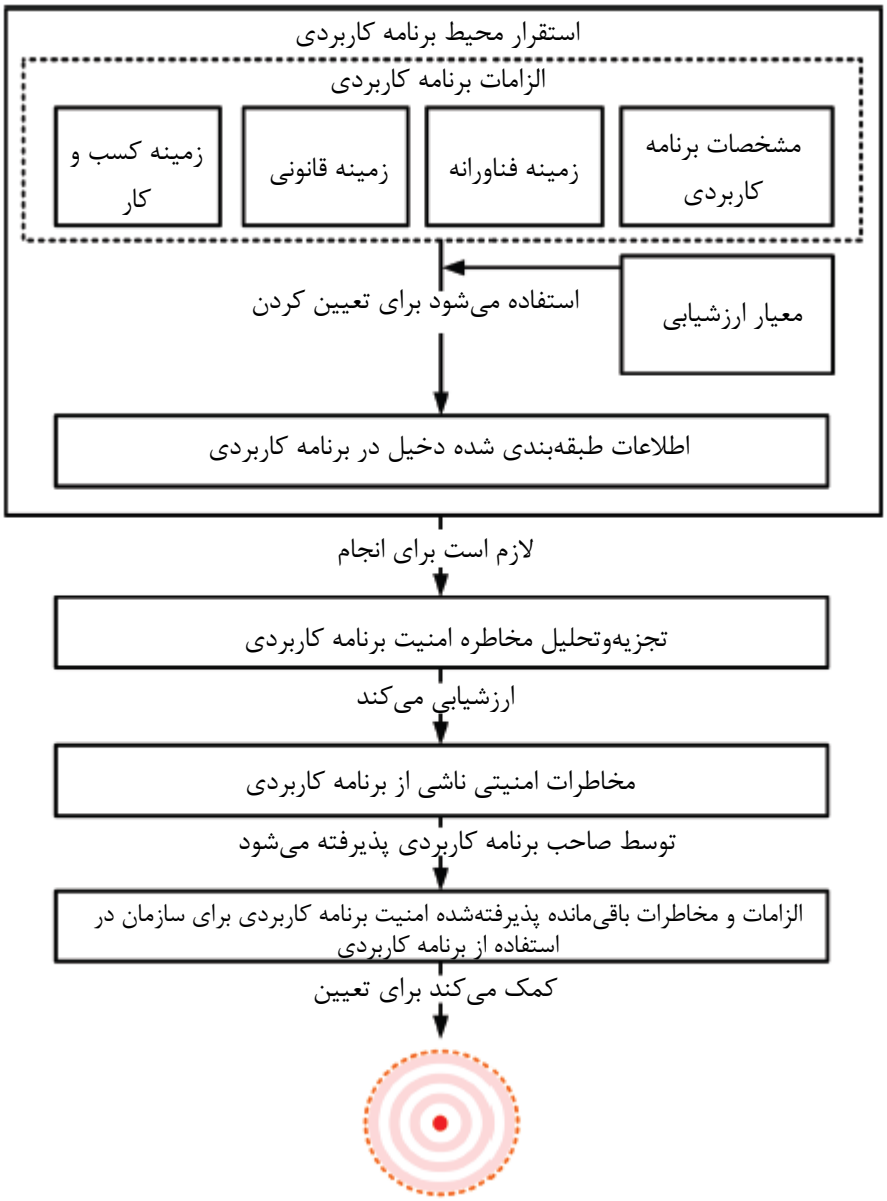
توصیه می‌شود خروجی فرایند تحلیل مخاطره امنیت برنامه کاربردی به شرح زیر باشد:

الف- فهرستی از مخاطرات امنیتی برای برنامه کاربردی و

ب- فهرستی از الزامات امنیتی برای برنامه کاربردی برای کاهش مخاطرات امنیتی.

این مورد باید مناسب کمک به گروه پروژه برای انتخاب ASCهای مناسب برای اشاره کردن به الزامات امنیتی یعنی انتخاب سطح اطمینان هدف برنامه کاربردی باشد.

شکل ۴ نشان می‌دهد که از چه لحاظی تحلیل مخاطره امنیت برنامه کاربردی، مرحله اساسی در تعیین سطح اطمینان هدف برنامه کاربردی محسوب می‌شود.



شکل ۴- تحلیل مخاطره امنیتی برنامه کاربردی به‌عنوان مرحله اساسی در تعیین سطح اطمینان هدف برنامه کاربردی

راهنمای بیشتر در مورد فرایند تحلیل مخاطره امنیت برنامه کاربردی در استاندارد ISO/IEC 27034-3 ارائه خواهد شد.

۵-۵-۱۳ فرایند درستی‌سنجی امنیت برنامه کاربردی

۵-۵-۱۳-۱ مقصود

مقصود این فرایند، اثبات سطح واقعی اعتماد برنامه کاربردی، در هر زمانی از چرخه‌عمر برنامه کاربردی است.

۵-۵-۱۳-۲ توصیف

فرایند ساده‌ای است که توسط آن گروه درستی‌سنجی، نتایج اندازه‌گیری‌های مربوط به درستی‌سنجی را برای هر یک از ASCهای مورد نیاز سطح اطمینان هدف برنامه کاربردی بررسی می‌کند.

۵-۵-۱۳-۳ نتایج

در نتیجه انجام این فرایند:

الف- سطح اطمینان واقعی برنامه کاربردی تعیین می‌شود و

ب- در صورتی که سطح واقعی برنامه کاربردی معادل با سطح اطمینان هدف است، مالک برنامه کاربردی شواهدی را مستندسازی می‌کند که مخاطره امنیت اطلاعات برای برنامه کاربردی، به سطح قابل قبولی کاهش یابد.

۵-۵-۱۳-۴ فعالیت‌های تحقق

جدول ۱۷- نمودار RACI در مورد تحقق فرایند درستی‌سنجی امنیت برنامه کاربردی

فعالیت‌های تحقق	مالک برنامه کاربردی	کارگروه ONF	گروه درستی‌سنجی	متخصص دامنه‌ای	ممیز
نتیجه سنجش درستی‌سنجی انجام شده توسط ممیز برای هر ASC مورد نیاز توسط برنامه کاربردی سطح هدف اعتماد به دست می‌آید، و مثبت بودن نتیجه درستی‌سنجی می‌شود.	A	I	R	C	C

۵-۵-۱۳-۴-۱ راهنما

فرایند درستی‌سنجی رسمی توسط خط‌مشی‌های درستی‌سنجی هدایت می‌شود که ممکن است هر زمانی طی چرخه عمر برنامه کاربردی انجام شود و توصیه می‌شود توسط گروه درستی‌سنجی مستقلی بدون دخالت در پروژه‌های برنامه کاربردی صورت گیرد.

توصیه می‌شود نتایج اندازه‌گیری‌های درستی‌سنجی برای هر ASC مورد نیاز توسط سطح اطمینان هدف برنامه کاربردی، به‌عنوان ورودی‌های مورد نیاز به‌دست آید.

ASCها اندازه‌گیری‌های درستی‌سنجی را توسط آزمون متنوع خط‌مشی‌ها مانند بازرسی، بازنگری و آزمون واحد تامین می‌کنند. دیگر رویکردهای درستی‌سنجی می‌توانند در مراحل بعدی چرخه عمر به‌عنوان آزمون جعبه سفید یا جعبه سیاه شامل آزمون یکپارچگی یا آزمون نفوذ استفاده شوند.

بازنگری این فرایند در استاندارد ISO/IEC 27034-1:2011، شکل ۱۴ ارائه می‌شود. توصیف تفصیلی فرایند درستی‌سنجی امنیت برنامه کاربردی موضوع استاندارد ISO/IEC 27034-4 بوده و راهنمای بیشتر در آن استاندارد بین‌المللی تامین خواهد شد.

پیوست الف

(آگاهی‌دهنده)

همسویی ONF و ASMP با استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207 از طریق استاندارد ISO/IEC 15026-4

الف-۱ کلیات

استاندارد ISO/IEC 15026-4[1] (سامانه‌ها و مهندسی نرم‌افزار- سامانه‌ها و تضمین نرم‌افزاری – قسمت ۴: تضمین در چرخه عمر) راهنما و توصیه‌هایی را برای هدایت فرایندها، فعالیت‌ها و وظایف مربوط به سامانه‌ها و محصولات نرم‌افزاری ارائه می‌دهد که به توجه خاصی به ادعاهای تضمینی برای خواص منتخب تحت عنوان خواص بحرانی نیاز دارد.

استاندارد ISO/IEC 15026-4 فهرست مستقل خواص فرایندها، فعالیت‌ها و وظایف را برای دستیابی به ادعا مشخص کرده و نتیجه این ادعا را نشان می‌دهد. در صورتی که ذینفعان توجه ویژه‌ای نسبت به خاصیت منتخب خاص و توجیه از طریق ادعای تضمینی را تعیین کنند، ASMP چارچوبی را برای نیل به ادعا تامین می‌کند.

الف-۲ نگاشت[2]

جدول نگاشت بندهای فرعی استاندارد ISO/IEC 15026-4، استاندارد ISO/IEC 15288 و بندهای فرعی استاندارد ISO/IEC 12207، عنصر ASMP و نقش عنصر ASMP در استاندارد ISO/IEC 15026 (همه قسمت‌ها) مربوط به فرایندهای بحرانی برای دستیابی به ادعای امنیت برنامه کاربردی را تامین می‌کند.

یادآوری ۱- با وجود اینکه همه فرایندها در استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207 در تلاش‌های توسعه دخیل هستند، این فرایندها واقعا در استاندارد ISO/IEC 15026 (همه قسمت‌ها) بحرانی محسوب می‌شوند که بیشتر به فرایندهای ONF و مدیریت آن مربوط می‌شود. مشابه با معیارهای انطباق در استاندارد ISO/IEC 15026 (همه قسمت‌ها)، توافقنامه، فرایندهای پروژه‌ای، فرایندهای فنی و فرایندهای خاص نرم‌افزاری استاندارد ISO/IEC 12207: 2008 انتظار می‌رود ولی بر این نگاشت تمرکزی صورت نمی‌گیرد.

یادآوری ۲- استاندارد ISO/IEC 27034-3 شامل فرایندهای امنیتی برنامه کاربردی و روابط اضافی بوده و همسو با فرایندهای مدیریتی و فنی در استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207 مطرح می‌شود.

یادآوری ۳- استاندارد ISO/IEC 27034-4 شامل فرایندهای درستی‌سنجی امنیت برنامه کاربردی می‌شود که سطح اطمینان واقعی برنامه کاربردی را اندازه‌گیری می‌کند.

---

[1] - استاندارد ملی ایران به شماره ۴-۱۶۳۴۳مربوط به سال ۲۰۱۲ موجود است.

2 - Mapping

جدول الف-۱- نگاشت بندهای فرعی استاندارد ISO/IEC 15026-4، استاندارد ISO/IEC 15288، استاندارد ISO/IEC 12207 و استاندارد ISO/IEC 27034

بند فرعی استاندارد ISO/IEC 15288	بند فرعی استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207	عنصر فرایند به ازای استاندارد ISO/IEC 27034-1	نقش عنصر ASMP در فرایندهای بحرانی استاندارد ISO/IEC 15026 همه قسمت‌ها
۷-۲ فعالیت اکتساب	ISO/IEC 15288:2008, 6.1.1 ISO/IEC 12207:2008, 6.1.1	۷-۳-۵ تدارک و عملیات برنامه کاربردی	اگر ASMP به منظور اکتساب برنامه کاربردی یا نرم‌افزار ایجاد شود، توصیه می‌شود که پروژه تضمین کند توافقنامه شیوه‌های امنیت برنامه کاربردی فرد خریدار انتظارات در کل چرخه عمر برای مولفه برنامه کاربردی را در نظر بگیرد. توصیه می‌شود ملاحظات مربوط به تدارک و عملیات برنامه کاربردی شامل انطباق با فرایندهای امنیتی کسب شونده (یا انتظارات فرایند) برای عنصر برنامه کاربردی اکتسابی، پذیرش معیارها، سازوکارهای تحویلی، امکان توافق طی تحویل، شناسایی ناهنجاری‌ها، شناسایی جعل در عنصر برنامه کاربردی هنگام ورود به مجموعه، انتظاراتی برای وضوح نقص و مدیریت وصله[1] و غیره.
۷-۳ فرایند عرضه	ISO/IEC 15288:2008, 6.1.2 ISO/IEC 12207:2008, 6.1.2	۷-۳-۵ تدارک و عملیات برنامه کاربردی	اگر ASMP برای برنامه کاربردی یا نرم‌افزار ایجاد شود و برای خریدار عرضه شود، توصیه می‌شود ASMP برای تضمین این مورد ایجاد شود که برای خریدار، محصول یا خدماتی را فراهم آورد که مطابق با الزامات مورد توافق است. توصیه می‌شود ملاحظات مربوط به تدارک و عملیات برنامه کاربردی شامل بازنگری فرایندهای امنیتی عرضه‌کننده برای عنصر برنامه کاربردی، مولفه خریداری شده، پذیرش معیارها، سازوکارهای تحویل، تشخیص ناهنجاری‌ها، شناسایی تقلب‌ها در وضوح نقص و مدیریت وصله و غیره شود.
۷-۴ فرایند طرح‌ریزی پروژه	ISO/IEC 15288:2008, 6.3.1 ISO/IEC 12207:2008, 6.3.1	۷-۳-۴ ایجاد و نگهداری چارچوب الزامی برنامه کاربردی	توصیه می‌شود فرایندهای طرح‌ریزی پروژه ASMP و ANF بعدی برای تعریف و نگهداری مدل چرخه عمر با بیشینه کاربرد استفاده شود که متشکل از مراحلی برای کاربرد در مدل‌های چرخه عمر امنیت برنامه کاربردی سازمان شود. در صورت پیاده‌سازی، فرایند مدیریت چرخه عمر توصیه می‌شود از ASMP برای ایجاد مدل‌های چرخه عمر

1 - Patch management

بند فرعی استاندارد ISO/IEC 15288	بند فرعی استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207	عنصر فرایند به ازای استاندارد ISO/IEC 27034-1	نقش عنصر ASMP در فرایندهای بحرانی استاندارد ISO/IEC 15026 همه قسمت‌ها
			استاندارد برای امنیت برنامه کاربردی سازمان بیشینه استفاده برده شود. توصیه می‌شود فرایند طرح‌ریزی پروژه، این‌گونه فرایندهای سازمانی را برای برآورده کردن نیازهای خاص پروژه متناسب کند.
۷-۵ فرایند مدیریت تصمیم‌گیری	ISO/IEC 15288:2008, 6.3.3 ISO/IEC 12207:2008, 6.3.3	۷-۳-۵ تدارک و عملیات برنامه کاربردی	فعالیت‌های فرایند مدیریت تصمیم‌گیری نیاز به تضمین این موضوع دارد که پیامدها و تاثیرات ناشی از امنیت برنامه کاربردی در زمان تصمیم‌گیری طی تدارک و عملیات برنامه کاربردی در نظر گرفته می‌شوند.
۷-۶ فرایند مدیریت مخاطره	ISO/IEC 15288:2008, 6.3.4 ISO/IEC 12207:2008, 6.3.4	۷-۳-۵ تدارک و عملیات برنامه کاربردی	توصیه می‌شود امنیت برنامه کاربردی مربوط به مخاطرات پروژه به‌طور کامل با فرایند مدیریت مخاطره برای تنظیم الویت‌ها، تصمیم‌گیری، ایجاد و نگهداری رخ‌نمون[1] مخاطره و طرز برخورد با مخاطره یکپارچه شود. توصیه می‌شود تدارک و عملیات برنامه کاربردی و مخاطره مربوط به شیوه واقعی در نظر گرفته شود که شامل مخاطرات اجبار به انجام دوباره در مورد قطعات برنامه کاربردی می‌شود. توصیه می‌شود پروژه پتانسیلی را به برای عدم توانایی در نیل به امنیت ضروری برنامه کاربردی مورد ارزشیابی قرار دهد که منجر به ارائه مدرک یا مجوز رسمی شده یا اینکه در نرم‌افزار طبق کاربرد در نظر گرفته شده، ارائه نشود.
۷-۷ مدیریت پیکربندی	ISO/IEC 15288:2008, 6.3.5 ISO/IEC 12207:2008, 6.3.5	۷-۳-۵ تدارک و عملیات برنامه کاربردی	فرایند مدیریت پیکربندی یکپارچگی همه مصنوعات پروژه یا فرایند شناسایی شده را برقرار کرده و نگهداری می‌کند و آن‌ها را برای طرفین مربوط قابل دسترس می‌گرداند. تدارک و عملیات برنامه کاربردی دارای دو رابطه مربوط به امنیت برنامه کاربردی است: ۱) مدیریت موثر پیکربندی مولفه‌های برنامه کاربردی برای تضمین امنیت برنامه کاربردی و ۲) اطلاعات ارائه دهنده دستاورد امنیت برنامه کاربردی که تحت مدیریت پیکربندی قرار دارند. یادآوری- راهنمای اضافی برای این نوع شیوه‌های مدیریت پیکربندی در استاندارد ISO/IEC 27002، فناوری اطلاعات –

[1] - Profile

بند فرعی استاندارد ISO/IEC 15288	بند فرعی استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207	عنصر فرایند به ازای استاندارد ISO/IEC 27034-1	نقش عنصر ASMP در فرایندهای بحرانی استاندارد ISO/IEC 15026 همه قسمت‌ها
			فنون امنیت- کد شیوه مربوط به واپایش‌های امنیت اطلاعات و استاندارد ISO 10007:2003، سامانه‌های مدیریت کیفیت- اصول راهنمای مدیریت پیکربندی قابل دسترس است.
۷-۸ فرایند مدیریت اطلاعات	ISO/IEC 15288:2008, 6.3.6 ISO/IEC 12207:2008, 6.3.6	۷-۳-۵ تدارک و عملیات برنامه کاربردی	برای امنیت برنامه کاربردی، فرایند مدیریت اطلاعات، اطلاعاتی را در مورد دستاورد امنیت برنامه کاربردی نسبت به ذینفعان مربوط، شامل مراجع نظارتی یا تاییدکننده فراهم می‌آورد.
۷-۹ فرایند تعریف الزامات ذینفعان	ISO/IEC 15288:2008, 6.4.1 ISO/IEC 12207:2008, 6.4.1	۷-۳-۲ تشخیص الزامات برنامه کاربردی و محیط آن	فرایند تعریف الزامات ذینفعان، الزاماتی را برای سامانه تعریف می‌کند که می‌تواند خدمات مورد نیاز کاربران و دیگر ذینفعان را در محیط تعریف شده‌ای فراهم آورد. فرایند مذکور این‌گونه خدمات را تحلیل نموده و به مجموعه عادی الزامات تغییر می‌دهد. به‌عنوان زیرمجموعه این‌گونه الزامات، سطح اطمینان هدف و خواص امنیتی برنامه کاربردی که برای درجه بالای اطمینان در موفقیت مورد نیاز است، شناسایی و مستندسازی می‌شود.
۷-۱۰ فرایند تحلیل الزامات	ISO/IEC 15288:2008, 6.4.2 ISO/IEC 12207:2008, 6.4.2	۷-۳-۳ ارزیابی مخاطرات امنیت برنامه کاربردی	فرایند تحلیل الزامات، دیدگاه ذینفع، الزام محور نسبت به خدمات دلخواه را به دیدگاه فنی محصول مورد نیاز تغییر می‌دهد که می‌تواند خدمات را در سطح اطمینان مورد هدف تحویل دهد. توصیه می‌شود تحلیل الزامات شامل ارزیابی مخاطرات امنیتی برنامه کاربردی و کفایت الزامات امنیت برنامه کاربردی مربوط باشد ولی به مرز کارکردی سامانه، کارکردهایی که سامانه برای اجرا نیاز دارد، محدودیت‌های ضروری پیاده‌سازی که توسط ذینفعان معرفی می‌شود یا محدودیت‌های غیرقابل اجتناب در راه‌حل، اندازه‌هایی که ارزیابی موفقیت فنی را امکان‌پذیر می‌سازد، محدود نمی‌شود.
۷-۱۱ فرایند درستی-سنجی	ISO/IEC 15288:2008, 6.4.6	۷-۳-۶ ممیزی امنیت برنامه کاربردی	در محتوای ASMP، فرایند درستی‌سنجی تایید می‌کند که سطح اطمینان مورد هدف خاص حاصل می‌شود. توصیه می‌شود نتایج، شامل اطلاعات مورد نیاز برای اقدامات مفیدی که موارد عدم انطباق‌ها در برنامه کاربردی محقق شده یا فرایندهایی را تصحیح می‌کند که بر مبنای آن عمل می‌کنند و عدم قطعیت را در فعالیت‌های درستی‌سنجی مانند قابلیت اطمینان ابزار

بند فرعی استاندارد ISO/IEC 15288	بند فرعی استاندارد ISO/IEC 15288 و استاندارد ISO/IEC 12207	عنصر فرایند به ازای استاندارد ISO/IEC 27034-1	نقش عنصر ASMP در فرایندهای بحرانی استاندارد ISO/IEC 15026 همه قسمت‌ها
			آزمون و سطح عدم قطعیت در نتایج، مورد توجه قرار می‌گیرد. (یعنی نرخ‌های مثبت کاذب و منفی کاذب) توصیه می‌شود ASM شواهد اعتبارسنجی ایجاد شده در کل چرخه عمر را در نظر گیرد. به‌عنوان مثال آزمون ضعف کد در فرایند توسعه یا طی حفظ سامانه.
۷-۱۲ فرایند عملیات	ISO/IEC 15288:2008, 6.4.9 ISO/IEC 12207:2008, 6.4.9	۷-۳-۵ تدارک و عملیات برنامه کاربردی	فرایند عملیات در ارتباط با تدارک و عملیات برنامه کاربردی به منظور تحویل خدمات در محیط مورد نظر بوده و حمایتی را برای مشتریان محصول نرم‌افزاری فراهم می‌آورد. توصیه می‌شود در مورد طرح‌هایی برای این فرایند، برای موفقیت امنیت برنامه کاربردی در کل عمر سامانه، محدودیت‌های عملیاتی و سازگاری فرضیاتی در رویکرد نسبت به امنیت برنامه کاربردی در نظر گرفته شود. توصیه می‌شود پروژه، سامانه‌های گزارش‌گیری و روش‌های اجرایی را برای بررسی و تعیین تکلیف امنیت برنامه کاربردی مربوط به حوادث ایجاد کند.
۷-۱۳ فرایند نگهداری	ISO/IEC 15288:2008, 6.4.10 ISO/IEC 12207:2008, 6.4.10	۷-۳-۵ تدارک و کاربرد برنامه کاربردی	در طرح‌هایی برای نگهداری طی تدارک و کاربرد برنامه کاربردی توصیه می‌شود امنیت در کل عمر سامانه در نظر گرفته شود. توصیه می‌شود پروژه تضمین کند که طرح نگهداری برای ارزشیابی تأثیر بر امنیت برنامه کاربردی در تغییرات صورت گرفته نسبت به مولفه‌های برنامه کاربردی یا سامانه طی نگهداری و شواهد مناسب دستیابی به سطح اطمینان مورد هدف فراهم می‌شود.

پیوست ب

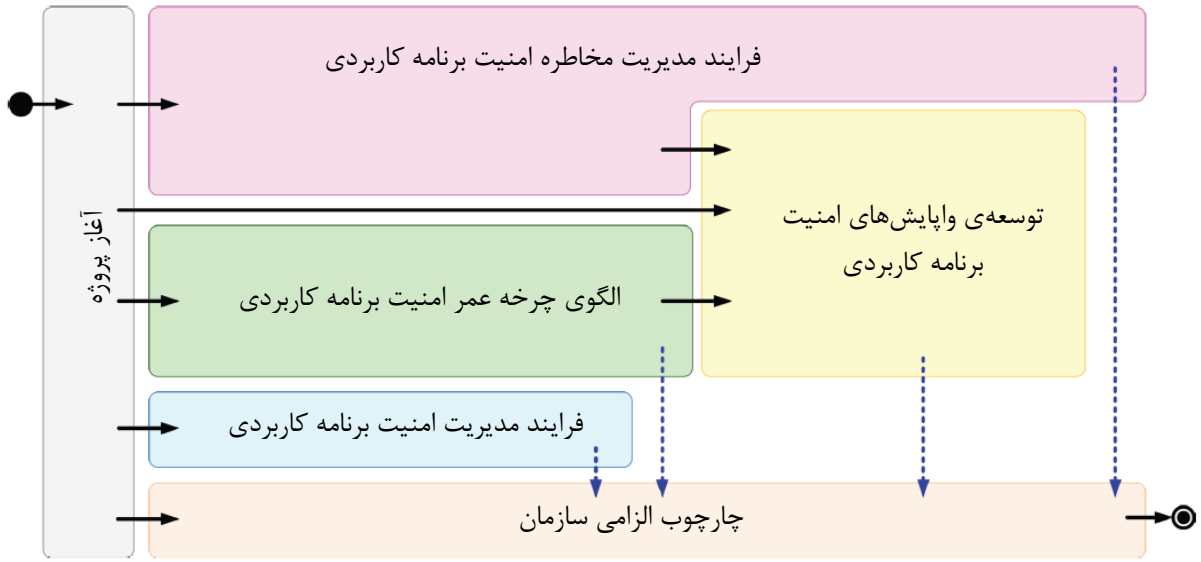
(آگاهی‌دهنده)

مثال پیاده‌سازی ONF: پیاده‌سازی استاندارد ISO/IEC 27034 مربوط به امنیت برنامه کاربردی و ONF مربوط در سازمان موجود

ب-۱ کلیات

در این مثال، موسسه مالی پروژه‌ای را برای پیاده‌سازی استاندارد امنیت برنامه کاربردی استاندارد ISO/IEC 27034 و ONF مربوط، برای بهبود امنیت برنامه‌های کاربردی و هماهنگ‌سازی مدیریت واپایش‌های امنیتی در کل پروژه‌های توسعه برنامه کاربردی، آغاز می‌کند.

همان‌گونه که در شکل ب-۱- به صورت طرحوار[1] نشان داده شده است، سازمان، پروژه را به شش زیرپروژه تقسیم می‌کند.



شکل ب-۱-پیاده‌سازی ONF در سازمان –مرورکلی زیرپروژه‌ها

ب-۱-۱ آغاز پروژه

ب-۱-۱-۱ مقصود

مقصود این زیرپروژه به صورت زیر مطرح می‌شود:

الف- تعریف حوزه و دامنه قابل قبول و قابل مدیریت برای پروژه و هر زیرپروژه

ب- تخصیص گروه‌های پروژه‌ای

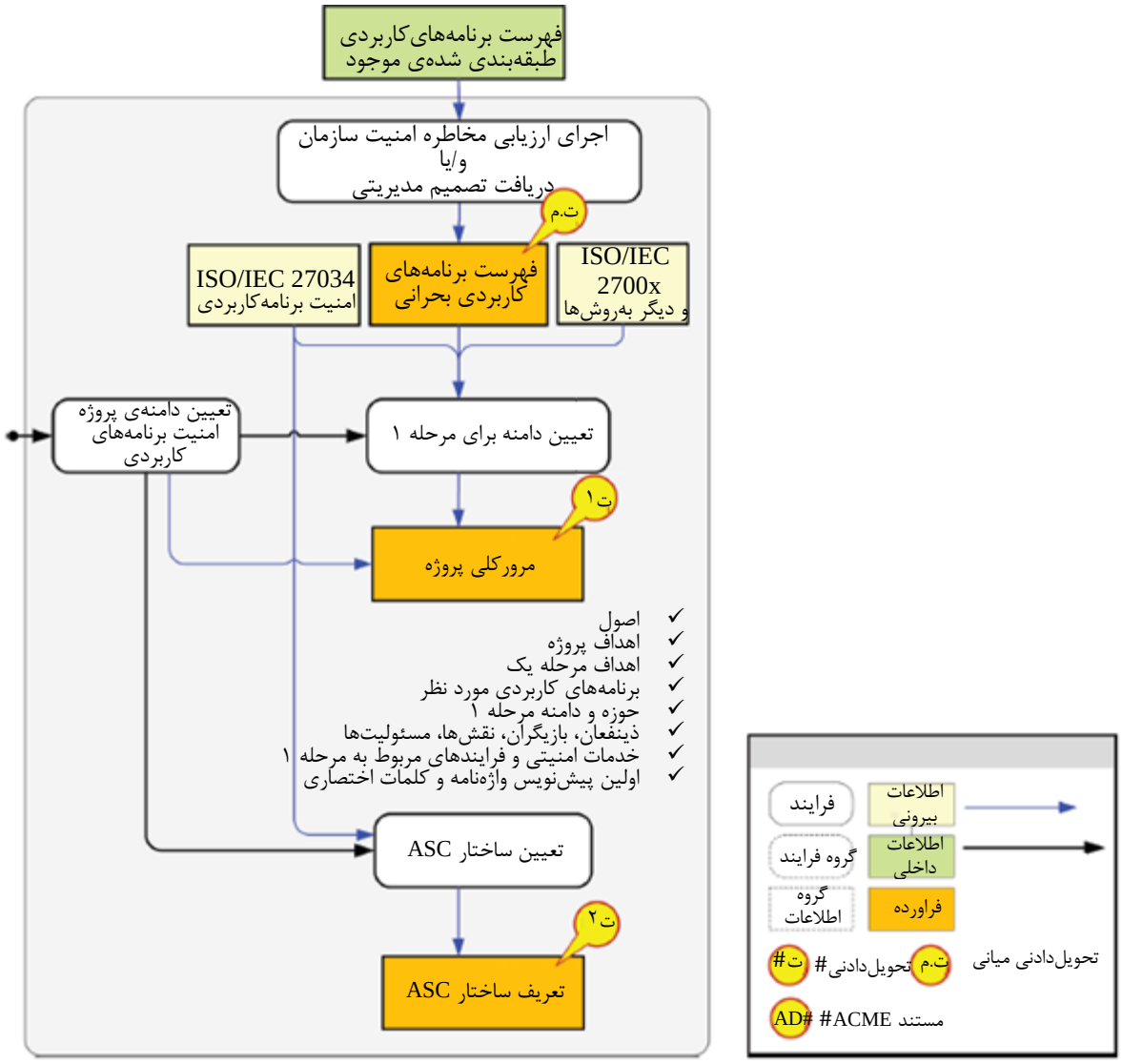
1 - Schematized

پ- تعیین ساختار ASCها که قرار است توسعه یابد و

ت- پایش زیرپروژه‌ها

ب-۱-۱-۲ مرورکلی زیرپروژه

شکل ب-۲ نمایش نگاشتاری زیرپروژه مورد نظر را نشان می‌دهد.



شکل ب-۲-پروژه پیاده‌سازی ONF در امنیت برنامه کاربردی، مرحله ۱

ب-۱-۱-۳ بازیگران

بازیگران درگیر این زیرپروژه عبارتند از:

الف- مدیریت در سطح بالا و

ب- مدیر پروژه

ب-۱-۱-۴ ورودی‌ها

ورودی این زیرپروژه‌ها، فهرستی از برنامه‌های کاربردی طبقه‌بندی شده موجود است (که توسط سامانه مدیریت امنیت اطلاعات فراهم شده است).

ب-۱-۱-۵ فعالیت‌ها

طبق شکل ب-۲ فعالیت‌های مربوط به زیرپروژه عبارتند از:

الف- تعریف حوزه و دامنه پروژه امنیت برنامه کاربردی؛

ب- اجرای ارزیابی مخاطره امنیت سازمان یا دریافت تصمیم مدیریت سطح بالا؛

پ- تعریف مرحله پروژه مذکور مطابق با قلم ب فوق و

ت- تعیین ساختار ASC.

ب-۱-۱-۶ نتایج

نتایج زیرپروژه موارد تحویلی زیر هستند:

الف- .iDiv - فهرست برنامه‌های کاربردی بحرانی

ب- Dlv 1– بازنگری پروژه برای تامین اطلاعات زیر:

۱- اصول

۲- اهداف پروژه

۳- اهداف مرحله ۱

۴- برنامه‌های کاربردی مورد نظر

۵- حوزه مرحله ۱

۶- ذینفعان، بازیگران، نقش‌ها، مسئولیت‌ها

۷- خدمات امنیتی و فرایندهای مربوط به مرحله ۱

۸- اولین پیش‌نویس واژه‌نامه و کلمات اختصاری

پ- Dlv 2– تعریف ساختار ASC

ب-۱-۲ زیرپروژه مدیریت مخاطره امنیتی مربوط به برنامه کاربردی

ب-۱-۲-۱ مقصود

طی انجام زیرپروژه، سازمان موارد زیر را طرح، حفظ نموده و از آن‌ها حمایت می‌کند:

الف- توسعه فرایند مدیریت مخاطره امنیتی برنامه کاربردی مطابق با بازیگران، مندرجات و مشخصات برنامه کاربردی

ب- تشخیص مخاطرات امنیتی با توجه به کاربرد برنامه‌های کاربردی بحرانی سازمان و

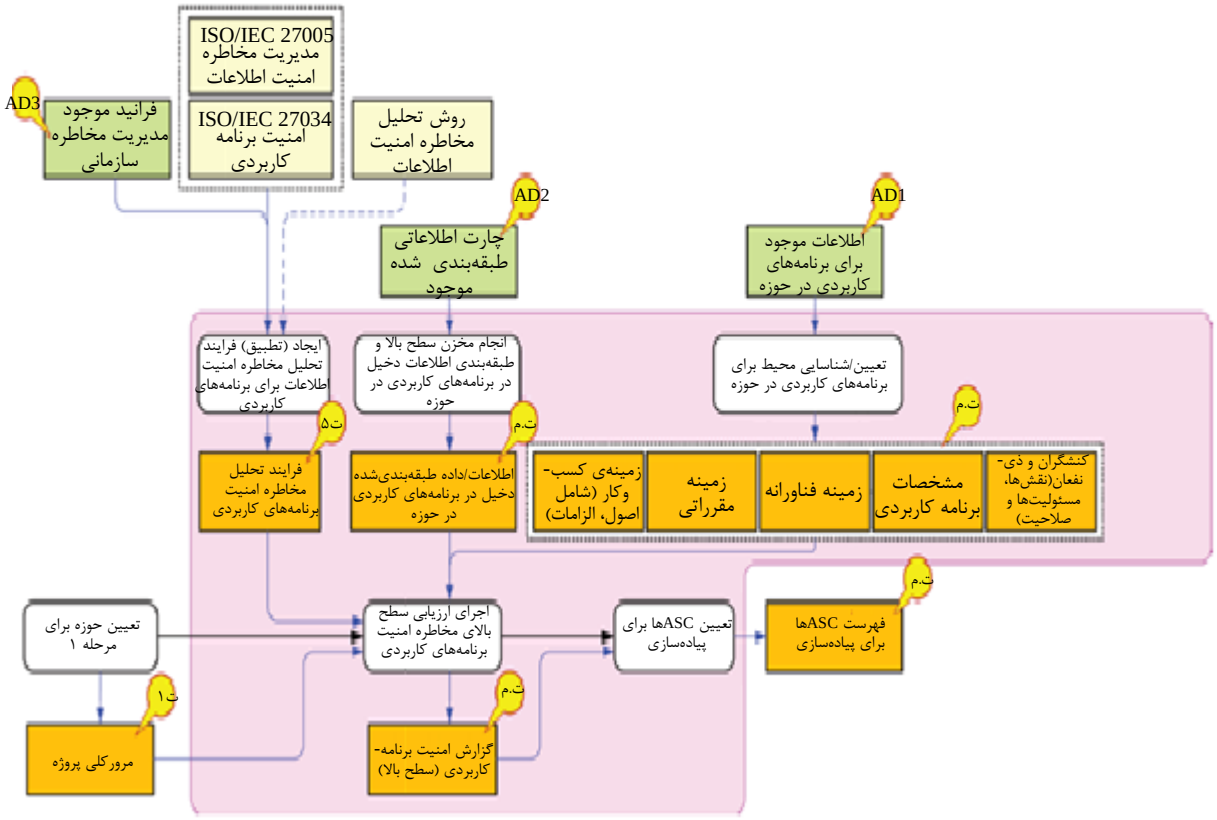
پ- تشخیص الزامات امنیتی که به ناچار توسط ASCها به آن رسیدگی می‌شود.

ب-۱-۲-۲ بازیگران

بازیگران دخیل در زیرپروژه، گروه مدیریت مخاطره امنیت فناوری اطلاعات محسوب می‌شوند.

ب-۱-۲-۳ بازنگری زیرپروژه

شکل ب-۳ نمایش نگاشتاری این زیرپروژه را نشان می‌دهد.



شکل ب-۳- زیرپروژه فرایند مدیریت مخاطره امنیت برنامه کاربردی

ب-۱-۲-۴ ورودی‌ها

ورودی‌های مربوط به این زیرپروژه عبارتند از:

الف- روش تحلیل مخاطره امنیت اطلاعات؛

ب- AD 1 – اطلاعات موجود برای برنامه‌های کاربردی مورد نظر؛

پ- AD2- نمودار اطلاعاتی طبقه‌بندی شده موجود؛

ت- -AD3 فرایند مدیریت مخاطره سازمانی موجود و

ث- ت۱- مرورکلی پروژه

ب-۱-۲-۵ فعالیت‌ها

فعالیت‌های مربوط به این زیرپروژه عبارتند از:

الف- ایجاد (تطابق) فرایند مخاطره امنیت اطلاعات برای برنامه‌های کاربردی؛

ب- شناخت مخزن سطح بالا و طبقه‌بندی اطلاعات در ارتباط با برنامه‌های کاربردی مورد نظر؛

پ- تعریف/ شناسایی محیطی برای برنامه‌های کاربردی مورد نظر؛

ت- اجرای ارزیابی مخاطره امنیت برنامه کاربردی سطح بالا و

ث- تعیین ASCهایی که قرار است به شرح زیر پیاده‌سازی شوند:

۱- تعریف فرایند انتخاب ASC؛

۲- الزامات امنیتی مرتبط با ASCها (مخاطره‌های امنیتی –> الزامات امنیتی –> ASCها).

ب-۱-۲-۶ نتایج

نتایج این زیرپروژه عبارتند از:

الف- Dvl 5- فرایند تحلیل مخاطره امنیت برنامه کاربردی

ب- i.Dvl- داده‌ها/ اطلاعات مرتبط طبقه‌بندی شده بر اساس برنامه‌های کاربردی مورد نظر

پ- i.Dlv- محیط برنامه‌های کاربردی عبارتند از:

۱- زمینه کسب‌وکار (شامل اصول، الزامات و غیره).

۲- زمینه مقرراتی.

۳- زمینه فناورانه.

۴- مشخصات برنامه‌های کاربردی.

۵- بازیگران و ذینفعان (نقش‌ها، مسئولیت‌ها و صلاحیت‌ها).

ت- i.Dlv- گزارش امنیت برنامه کاربردی (سطح بالا).

ث- i.Dlv- فهرست ASCهایی که قرار است پیاده‌سازی شوند.

ب-۱-۳ زیرپروژه مدل چرخه عمر برنامه کاربردی

ب-۱-۳-۱ مقصود

طی این زیرپروژه سازمان موارد زیر را طرح کرده، انجام داده و از آن‌ها حمایت خواهد کرد:

الف- هماهنگ‌سازی روش‌ها، فرایند و فعالیت‌های موجود در چرخه‌های مختلف عمر سازمان

ب- همکاری مدیریت پاسخگوی مناسب و گروه‌های دخیل در حاکمیت[1]، معماری، انطباق، توسعه، عملیات، فناوری اطلاعات، درستی‌سنجی و ممیزی و

پ- تعیین مراحل چرخه عمر در حوزه و دامنه مرحله ۱

ب-۱-۳-۲ بازیگران

بازیگران مربوط به زیرپروژه مذکور عبارتند از:

الف- گروه شیوه‌های انطباق؛

ب- گروه شیوه‌های توسعه برنامه کاربردی در زمینه فناوری اطلاعات؛

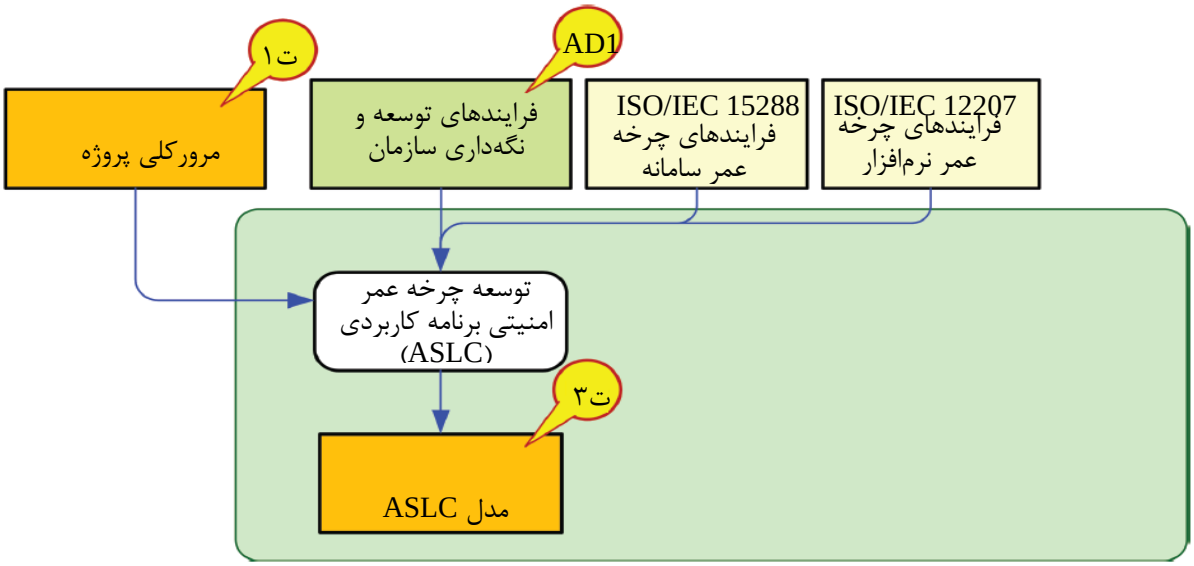
پ- حاکمیت و گروه شیوه‌های مدیریت پروژه؛

ت- یکپارچگی امنیتی در گروه پروژه‌ها و

ث- گروه شیوه‌های معماری امنیتی.

ب-۱-۳-۳ بازنگری زیرپروژه

شکل ب-۴ نمایش نگاشتاری این زیرپروژه را نشان می‌دهد.



شکل ب-۴-زیرپروژه مدل چرخه عمر امنیت برنامه کاربردی

1 - Governance

ب-۱-۳-۴ ورودی‌ها

ورودی‌های مربوط به این زیرپروژه عبارتند از:

الف- AD 1: فرایندهای توسعه و نگهداری سازمان و

ب- Dlv1- بازنگری پروژه

ب-۱-۳-۵ فعالیت‌ها

فعالیت مربوط به این زیرپروژه عبارت است از: توسعه چرخه عمر امنیت برنامه کاربردی ASLC برای سازمان

ب-۱-۳-۶ نتایج

نتیجه این زیرپروژه عبارت است از: مدل Dlv 3-ASLC

ب-۱-۴ زیرپروژه فرایند مدیریت امنیت برنامه کاربردی

ب-۱-۴-۱ مقصود

طی این زیرپروژه، سازمان فرایند مدیریت امنیت برنامه کاربردی را در تطابق با سازمان و سازگاری با الزامات استاندارد ISO/IEC 27034 طرح‌ریزی کرده، انجام داده و از آن محافظت خواهد کرد.

ب-۱-۴-۲ بازیگران

بازیگران این زیرپروژه عبارتند از:

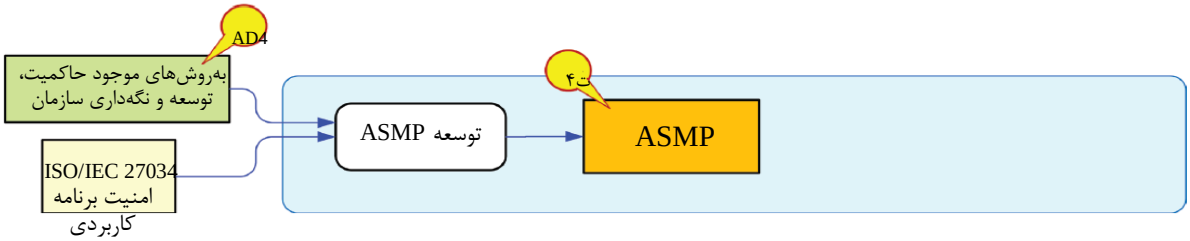
الف- گروه شیوه‌های توسعه نرم‌افزاری؛

ب- گروه شیوه‌های حاکمیت و مدیریت پروژه و

پ- یکپارچگی امنیتی در گروه پروژه‌ها.

ب-۱-۴-۳ بازنگری زیرپروژه

شکل ب-۵ نمایش نگاشتاری این زیرپروژه را نشان می‌دهد.



شکل ب-۵- زیرپروژه فرایند مدیریت امنیت برنامه کاربردی

ب-۱-۴-۴ ورودی‌ها

ورودی مربوط به این زیرپروژه عبارت است از: AD 4- شیوه‌های حاکمیت، توسعه و نگهداری به‌کار رفته توسط سازمان موجود

ب-۱-۴-۵ فعالیت‌ها

فعالیت مربوط به زیرپروژه مذکور عبارت است از: توسعه فرایند مدیریت امنیت برنامه کاربردی سازمان

ب-۱-۴-۶ نتایج

نتیجه این زیرپروژه عبارت است از: Dlv 4-ASMP (مستندسازی و راهنمایی برای یکپارچگی امنیت برنامه کاربردی در پروژه)

ب-۱-۵ زیرپروژه چارچوب الزامی سازمان

ب-۱-۵-۱ مقصود

طی این زیرپروژه، سازمان موارد زیر را طرح‌ریزی کرده، انجام داده و از آن محافظت خواهد کرد.

الف- نامزدی اعضای کارگروه ONF؛

ب- توسعه فرایندهای مدیریت و نگهداری ONF و

پ- ترکیب عناصر امنیت برنامه کاربردی در مخزن معتبر، قابل دسترس برای همه موارد قابل ملاحظه

ب-۱-۵-۲ بازیگران

بازیگران دخیل در این زیرپروژه عبارتند از:

الف- گروه شیوه‌های انطباق

ب- گروه شیوه‌های توسعه برنامه کاربردی در زمینه فناوری اطلاعات

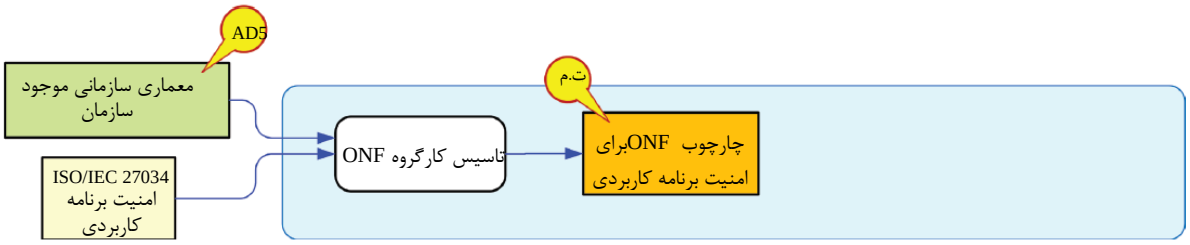
پ- گروه شیوه‌های حاکمیت و مدیریت پروژه

ت- گروه شیوه‌های عملیات و زیرساخت فناوری اطلاعات و

ث- حاکمیت- گروه حمایت از مدیریت پروژه

ب-۱-۵-۳ مرورکلی زیرپروژه

شکل ب-۶ نمایش نگاشتاری این زیرپروژه را نشان می‌دهد.



شکل ب-۶- زیرپروژه چارچوب الزامی سازمان

ب-۱-۵-۴ ورودی‌ها

ورودی مربوط به زیرپروژه عبارت است از: معماری سازمانی موجود سازمان

ب-۱-۵-۵ فعالیت‌ها

فعالیت مربوط به این زیرپروژه عبارت است از: تاسیس کارگروه ONF

ب-۱-۵-۶ نتایج

فعالیت مربوط به این زیرپروژه عبارت است از: i-Dlv- چارچوب الزامی سازمان برای امنیت برنامه کاربردی

ب-۱-۶ زیرپروژه توسعه واپایش‌های امنیت برنامه‌های کاربردی

ب-۱-۶-۱ مقصود

طی زیرپروژه، سازمان از موارد زیر طرح‌ریزی کرده، انجام داده، از آن‌ها نگهداری، حمایت کرده و ممیزی می‌کند:

الف- توسعه ASCها مطابق با الزامات امنیت برنامه کاربردی سازمان؛

ب- اعتبارسنجی، درستی‌سنجی، آزمون، پیاده‌سازی و ممیزی ASCهای توسعه‌یافته؛

پ- همسویی ASCها با مدل چرخه عمر امنیت برنامه کاربردی؛

ت- مدیریت فرایند نگهداری و توسعه ASC؛

ث- توسعه آموزش برای افرادی که ASCها را توسعه داده و اعتبار خواهند بخشید و

ج- توسعه آموزش برای افرادی که پیاده‌سازی، درستی‌سنجی و ممیزی ASCها انجام خواهند داد.

ب-۱-۶-۲ بازیگران

بازیگران دخیل در این زیرپروژه عبارتند از:

الف- مالکان برنامه‌های کاربردی موردنظر؛

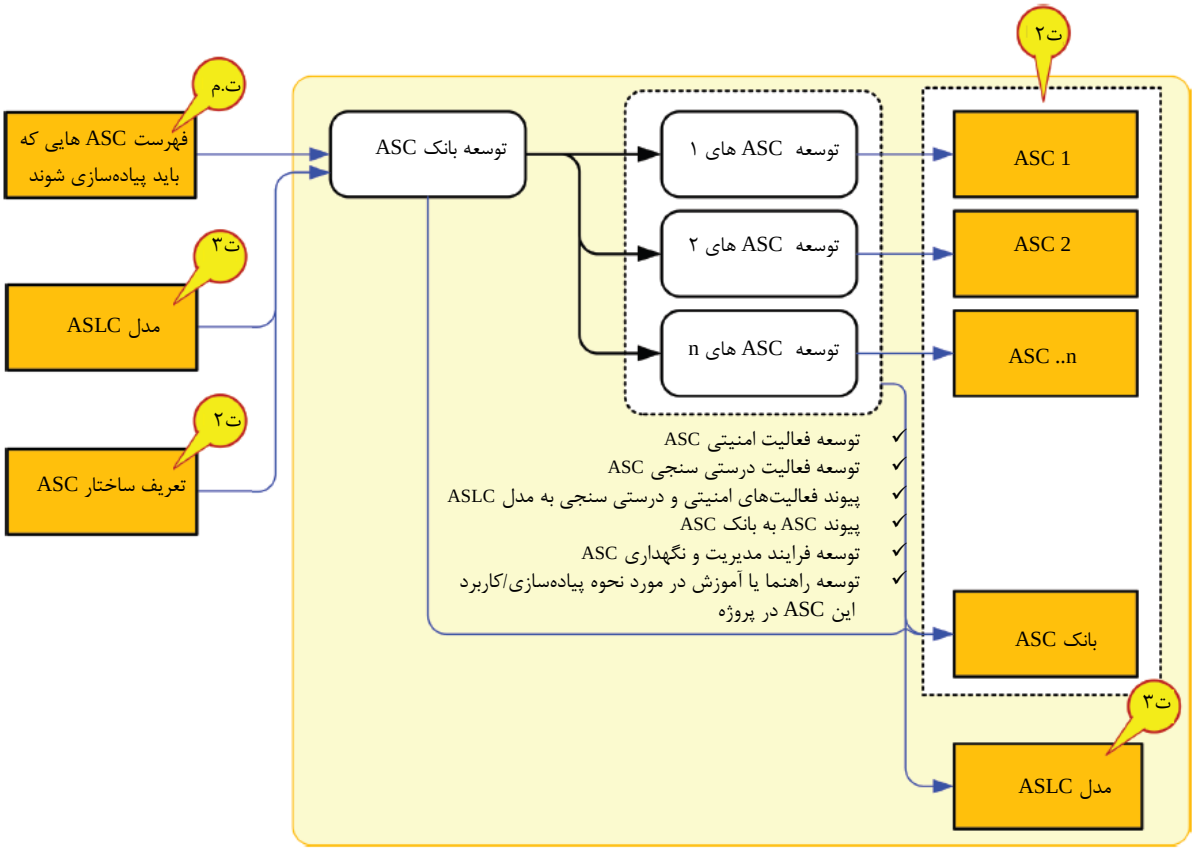
ب- گروه شیوه‌های انطباق- گروه چارچوب واپایش‌های امنیت اطلاعات؛

پ- گروه شیوه‌های توسعه نرم‌افزاری و

ت- گروه شیوه‌های توسعه برنامه کاربردی در زمینه فناوری اطلاعات.

ب-۱-۶-۳ بازنگری زیرپروژه

شکل ب-۷ نمایش نگاشتاری این زیرپروژه را نشان می‌دهد.



شکل ب-۷- زیرپروژه توسعه واپایش‌های امنیت برنامه‌های کاربردی

ب-۱-۶-۴ ورودی‌ها

ورودی‌های مربوط به این زیرپروژه عبارتند از:

الف- i.Dlv- فهرست ASCهایی که قرار است پیاده‌سازی شوند؛

ب- Dlv 2- تعریف ساختار ASC و

پ- Dlv 3- مدل ASLC.

ب-۱-۶-۵ فعالیت‌ها

فعالیت‌های مربوط به این زیرپروژه عبارتند از:

الف- توسعه بانک ASC

ب- توسعه ASCهای از شماره ۱،۲ الی n:

۱- توسعه فعالیت امنیتی ASC؛

۲- توسعه فعالیت درستی‌سنجی ASC؛

۳- پیوند فعالیت‌های امنیتی و درستی‌سنجی به مدل ASLC؛

۴- پیوند ASC به بانک ASC؛

۵- توسعه فرایند مدیریت و نگهداری ASC و

۶- توسعه راهنما یا آموزش در مورد نحوه پیاده‌سازی / کاربرد این ASC در پروژه.

ب-۱-۶-۶ نتایج

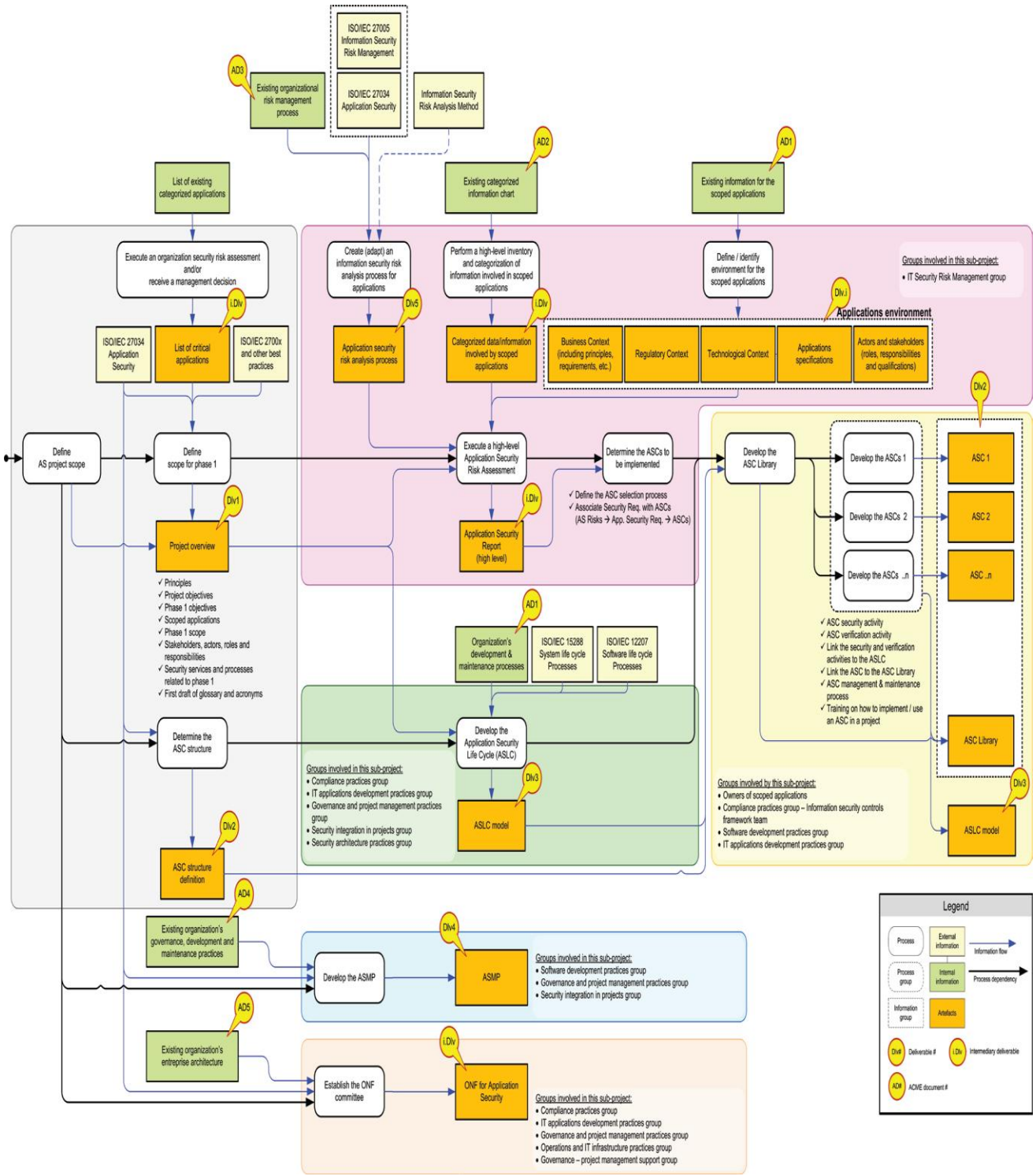
نتایج به‌دست آمده از این زیرپروژه عبارتند از:

الف- ASCها؛

ب- بانک ASC و

پ- Dlv 3- مدل ASLC (به‌روزرسانی شده).

ب-۲ نگاشتار گردش کار کامل پروژه



شکل ب-۸- مثال پیاده‌سازی ONF: پیاده‌سازی امنیت برنامه کاربردی استاندارد ISO/IEC 27034 و ONF مربوط در سازمان- نمودار مرورکلی

کتاب‌نامه

[1] ISO 9000, Quality management systems — Fundamentals and vocabulary

[2] ISO/IEC/TS 15504-8, Information technology — Process assessment — Part 8: An exemplar process assessment model for IT service management

[3] ISO 19011, Guidelines for auditing management systems

[4] ISO/IEC 20000-2, Information technology — Service management — Part 2: Guidance on the application of service management systems

[5] ISO/IEC 20000-3, Information technology — Service management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1

[6] ISO/IEC/TR 20000-4, Information technology — Service management — Part 4: Process reference model

[7] ISO/IEC/TR 20000-5, Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1

[8] ISO/IEC/TR 20000-9, Information technology — Service management — Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services

[9] ISO/IEC/TR 90006, Information technology — Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011

[10] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[11] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance

[12] ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement

[13] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[14] ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[15] ISO/IEC 27007, Information technology — Security techniques — Guidelines for information security management systems auditing

[16] ISO/IEC/TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls

[17] ISO/IEC 27010, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

[18] ISO/IEC 27014, Information technology — Security techniques — Governance of information security

[19] ISO 31000, Risk management — Principles and guidelines

[20] ISO Guide 73:2009, Risk management — Vocabulary