INSO-ISO-IEC

27036-3

1st. Edition

2015

Identical with
ISO/IEC 27036-3:
2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران-
ایزو- آی ای سی

۲۷۰۳۶-۳
چاپ اول

۱۳۹۳

فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط تأمین‌کننده – قسمت ۳: راهنماهایی برای امنیت زنجیره تأمین فناوری اطلاعات و ارتباطات

Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization

2 - International Electrotechnical Commission

3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط تأمین‌کننده قسمت ۳: راهنماهایی برای امنیت زنجیره تأمین فناوری اطلاعات و ارتباطات»

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤول سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی)	مدیرکل سازمان فناوری اطلاعات ایران
اعضاء : (اسامی به ترتیب حروف الفبا)	
بخشایش، سعید (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت فناوران توسعه امن ناجی
آریا، بهناز (دکتری مهندسی کامپیوتر)	قائم مقام مؤسسه کهکشان نور
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
جمیل‌پناه، ناصر (فوق لیسانس کامپیوتر)	کارشناس ارشد حوزه مخابرات
مغانی، مهدی (فوق لیسانس ریاضی کاربردی)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
ناظمی، اسلام (دکترای مهندسی کامپیوتر نرم‌افزار)	استادیار دانشگاه شهید بهشتی

نصیری آسایش، حمید رضا پژوهش‌گر دانشگاه شهید بهشتی
(فوق لیسانس فناوری اطلاعات معماری سازمانی)

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

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط تأمین‌کننده قسمت ۳: راهنماهایی برای امنیت زنجیره تأمین فناوری اطلاعات و ارتباطات» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و شصت و دومین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۳/۱۱/۲۹ مورد تصویب قرار گرفته است ، اینک 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 می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین ، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

منبع و مآخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC 27036-3: 2014, Information Technology — Security Techniques — Information Security for Supplier Relationships— Part ۳: Guidelines for information and communication technology supplychain security

فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط تأمین‌کننده

قسمت ۳: راهنماهایی برای امنیت زنجیره تأمین فناوری اطلاعات و ارتباطات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنماهایی برای کارفرمایان و تأمین‌کنندگان زنجیره تأمین اطلاعات فناوری اطلاعات و ارتباطات(ICT)[1] در رابطه با موارد زیر است:

الف) دستیابی به مشاهده‌پذیری و مدیریت مخاطرات امنیت اطلاعاتی که به دلیل زنجیره‌های تأمین اطلاعات ICT چندلایه که به صورت فیزیکی پراکنده هستند ایجاد شده‌اند.

ب) پاسخگویی به مخاطرات ناشی از زنجیره تأمین ICT جهانی در محصولات و خدمات ICT که می‌تواند به‌وسیله این محصولات و خدمات بر روی امنیت اطلاعات سازمان تأثیرگذار باشد. این مخاطرات می‌توانند علاوه بر جنبه‌های فنی به جنبه‌های سازمانی نیز مربوط باشند(مانند درج کد مخرب یا وجود محصولات تقلبی فناوری اطلاعات (IT)[2])؛

پ) یکپارچه‌سازی فرایندها و روش‌های اجرایی امنیت اطلاعات در فرایندهای چرخه حیات سامانه‌ها و نرم‌افزارهایی که در ISO/IEC 15288 و ISO/IEC 12207 توضیح داده شده‌اند همزمان با پشتیبانی از کنترل‌های امنیت اطلاعاتی که در استاندارد ISO/IEC 27002 شرح داده شده‌اند.

این قسمت از استاندارد ملی INSO-ISO/IEC 27036 مسائل مربوط به مدیریت/بازگشت‌پذیری[3] استمرار کسب‌وکار که در زنجیره تأمین ICT وجود دارند را شامل نمی‌شود. استاندارد ملی شماره ۲۷۰۳۱ مسائل استمرار کسب‌وکار را در بر می‌گیرد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شوند. درصورتی‌که به مدرکی با بیان تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون بیان تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها موردنظر است.

1- Information and Communication Technology
2- Information Technology
3- resiliency

استفاده از مراجع زیر[1] برای این استاندارد الزامی است:

2-1 ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*
2-2 ISO/IEC 27036-1, Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts
2-3 ISO/IEC 27036-2, Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین‌شده در استاندارد ISO/IEC 27000 و استاندارد ISO/IEC 27036-1 اصطلاحات و تعاریف زیر نیز به کار می‌رود:

۳-۱

اطمینان‌پذیری[2]

. ویژگی یک سامانه و قسمت‌های آن برای انجام دقیق مأموریت مورد نظر، بدون شکست[3] یا تنزل[4] چشمگیر است.

۳-۲

عنصر سامانه[5]

عضوی از مجموعه عناصری است که سامانه را تشکیل می‌دهند.

یادآوری- عنصر سامانه، قسمت مجزایی از سامانه است که می‌تواند برای تحقق الزامات مشخص‌شده استفاده شود. عنصر سامانه می‌تواند سخت‌افزار، نرم‌افزار، داده، نیروی انسانی، فرایندها (مانند فرایندهایی که کارکردهای لازم برای کاربران را فراهم می‌کنند)، رویه‌ها[6] (مانند دستورالعمل‌های عملگر) تسهیلات، مواد و موجودیت‌های طبیعی (مانند آب، اعضاء و مواد معدنی باشد) یا هر ترکیبی از آن‌ها باشد.

۳-۳

شفافیت[7]

خصوصیتی از سامانه یا فرایند است که بیانگر باز بودن و پاسخگویی است.

---

۱ - استاندارد بین‌المللی ISO/IEC 27000 در سال ۱۳۹۱ با شماره ملی ۲۷۰۰۰ منتشر شده است.

2- Reliability
3- Failure
4 - Degradation
5- System
6 - Procedures
7- Transparency

۴-۳

قابلیت ردیابی[1]

خصوصیتی است که اجازه ردگیری فعالیت یک شناسه، فرایند، یا عنصر را در زنجیره تأمین فراهم می‌کند.

۵-۳

اعتبارسنجی[2]

تأیید از طریق فراهم کردن مدارک مربوط به هدف است، که مشخص می‌کند الزامات مربوط به یک هدف یا برنامه کاربردی خاص فراهم شده‌اند.

یادآوری- تأیید برآورده شدن الزامات برای یک استفاده یا کاربرد خاص مورد نظر، از طریق فراهم آوردن شواهد عینی، صحه‌گذاری نامیده می‌شود.

[استاندارد ملی ایران شماره ۱۶۳۰۴ : سال ۱۳۹۱، تعریف ۴-۳۷]

۶-۳

درستی‌سنجی[3]

تأیید از طریق فراهم کردن مدارک مربوط به هدف است، که مشخص می‌کند الزامات مشخص‌شده فراهم شده‌اند یا خیر.

یادآوری- تأیید برآورده شدن الزامات تعیین‌شده، از طریق فراهم آوردن شواهد عینی، تصدیق نام دارد.

[استاندارد ملی ایران شماره ۱۶۳۰۴ : سال ۱۳۹۱، تعریف ۴-۳۸]

۴ ساختار این استاندارد

ساختار این استاندارد به‌گونه‌ای است که با ISO/IEC 15288 و ISO/IEC 12207 هماهنگ باشد. بند ۶ فرایندهای چرخه حیات فراهم‌شده در این دو استاندارد را منعکس می‌کند. این استاندارد، همچنین با استاندارد ISO/IEC 27002 هماهنگ بوده و با نگاشت فراهم‌شده در پیوست ب، به کنترل‌های امنیت اطلاعات مرتبط در فرایندهای چرخه حیات ارجاع می‌دهد.

مستنداتی که در این استاندارد از آن‌ها نام برده می‌شود عمومی بوده و نیاز به تشریح یا مستندات جداگانه ندارند سازمان‌ها باید از مستندات موجود برای یکپارچه کردن امنیت زنجیره تأمین ICT استفاده کنند.

۵ مفاهیم کلیدی

1- Traceability
2- Validation
3- Verification

۵-۱ مورد کسب‌وکاری برای امنیت زنجیره تأمین ICT

سازمان‌ها محصولات و خدمات ICT را از تأمین‌کنندگان مختلفی اکتساب می‌کنند که آن‌ها نیز ممکن است به‌نوبه خود مؤلفه‌هایی را از دیگر تأمین‌کنندگان اکتساب کنند. مخاطرات امنیت اطلاعات مربوط به این زنجیره‌های تأمین ICT پراکنده و چندلایه می‌تواند به‌وسیله کاربردهای روش‌های اجرایی مدیریت مخاطرات و روابط مورد اطمینان مدیریت‌شده و به این وسیله مشاهده‌پذیری، ردیابی و شفافیت در زنجیره تأمین ICT افزایش یابد.

به‌عنوان‌مثال، مشاهده‌پذیری در زنجیره تأمین ICT از طریق تعریف الزامات کافی برای امنیت اطلاعات و کیفیت و پایش مستمر تأمین‌کنندگان و محصولات و خدمات آن‌ها پس از عملیاتی شدن رابطه تأمین‌کننده به دست می‌آید. شناسایی و ردگیری افراد مسئول برای کیفیت و امنیت عناصر حیاتی قابلیت ردیابی بیشتری را فراهم می‌کند. ایجاد الزامات و انتظارات قراردادی در کنار بازنگری فرایندها و روش‌های اجرایی شفافیت بیشتری را فراهم می‌آورد.

کارفرمایان، باید درکی درباره مخاطرات زنجیره تأمین ICT و تأثیر آن‌ها بر کسب‌وکار خود را در سازمان ایجاد کنند. مشخصاً مدیریت سازمان کارفرما باید آگاه باشد که روش‌های اجرایی تأمین‌کننده در سراسر زنجیره تأمین می‌تواند در این‌که محصولات و خدمات ارائه‌شده از سوی تأمین‌کننده برای محافظت از کسب‌وکار، اطلاعات و سامانه‌های اطلاعاتی کارفرما قابل اطمینان هستند تأثیرگذار باشند.

۵-۲ مخاطرات زنجیره تأمین ICT و تهدیدهای مرتبط با آن

در یک زنجیره تأمین، مدیریت امنیت اطلاعات یک سازمان منفرد (کارفرما یا تأمین‌کننده) برای نگهداشت امنیت اطلاعات محصولات و خدمات ICT در سراسر زنجیره تأمین اطلاعات کافی نیست. مدیریت منابع تأمین‌کنندگان، محصولات و خدمات توسط کارفرما برای امنیت اطلاعات ضروری است.

اکتساب محصولات و خدمات ICT مخاطرات خاصی را در قالب مدیریت مخاطرات امنیت اطلاعات برای کارفرما مطرح می‌کند. با پراکنده‌تر شدن زنجیره‌های تأمین ICT به صورت فیزیکی، و پیمایش مرزهای جهانی و سازمانی، ردیابی روش‌های اجرایی تولید و عملیات خاصی که در عناصر منفرد ICT (محصولات، خدمات و مؤلفه‌های آن‌ها) به کار گرفته می‌شوند بسیار مشکل‌تر می‌شود. این ردیابی شامل شناسایی افراد مسئول برای کیفیت و امنیت عناصر بیان‌شده است. این دشواری، کمبود ردیابی در زنجیره تأمین ICT را ایجاد کرده و این موجب مخاطرات بالاتر زیر می‌شود:

- به مخاطرات انداختن امنیت اطلاعات و در نتیجه عملیات کسب‌وکار کارفرما از طریق وقایع عمدی مانند درج کد مخرب و ارائه محصولات تقلبی در زنجیره تأمین ICT
- وقایع غیرعمدی مانند روش‌های اجرایی نامنظم توسعه نرم‌افزار

هر دو دسته وقایع عمدی و غیرعمدی می‌توانند به مخاطرات افتادن داده‌ها و عملیات کارفرما شامل سرقت

دارایی معنوی، نشت داده[1]، و کاهش توانایی کارفرما در انجام کارکردهای کسب‌وکار را به همراه داشته باشند. هر یک از این موارد شناسایی‌شده در صورت وقوع می‌تواند به شهرت سازمان آسیب زده و تأثیرات بعدی مانند از دست دادن کسب‌وکار را به همراه داشته باشد.

۵-۳ انواع روابط کارفرما و تأمین‌کننده

ممکن است کارفرمایان و تأمین‌کنندگان محصولات و خدمات ICT موجودیت‌های مختلفی را در روابط مختلف مبتنی بر زنجیره تأمین درگیر کنند. این روابط شامل موارد زیر بوده اما به این موارد محدود نمی‌شود:

الف) پشتیبانی مدیریت سامانه ICT در جایی که مالکیت سامانه با کارفرما بوده و مدیریت آن با تأمین‌کننده.

ب) فراهم‌کنندگان سامانه‌ها یا خدمات ICT در جایی مالکیت و مدیریت سامانه یا منابع با تأمین‌کننده است.

پ) توسعه، طراحی، مهندسی و ساخت محصول در جایی که تأمین‌کننده تمام یا قسمت‌هایی از خدمت مربوط به ایجاد محصولات ICT را فراهم می‌کند.

ت) تأمین‌کنندگان محصولات آماده تجاری

ث) تأمین‌کنندگان و توزیع‌کنندگان محصولات متن‌باز

سطح مخاطرات و نیاز به اعتماد از سوی کارفرما در روابط تأمین‌کننده با اعطای دسترسی بیشتر به تأمین‌کننده در زمینه دسترسی به اطلاعات و سامانه‌های اطلاعاتی کارفرما و وابستگی بیشتر کارفرما به محصولات و خدمات تأمین‌کننده افزایش می‌یابد. برای مثال، اکتساب پشتیبانی مدیریت سامانه ICT در برخی از مواقع مخاطرات بالاتری از محصولات آماده تجاری یا متن‌باز دارد. از دیدگاه تأمین‌کننده، هر گونه افشای غیرمجاز اطلاعات کارفرما می‌تواند به شهرت تأمین‌کننده و اعتماد کارفرمایی که اطلاعات و سامانه‌های اطلاعاتی وی به خطر افتاده است ایجاد کند.

برای کمک به مدیریت عدم قطعیت و مخاطرات مربوط به روابط تأمین‌کننده، توصیه می‌شود که کارفرمایان و تأمین‌کنندگان گفتمان و تحقیقی در مورد درک انتظارت متقابل درباره محافظت از اطلاعات و سامانه‌های اطلاعاتی یکدیگر ایجاد کنند.

۵-۴ قابلیت سازمانی

توصیه می‌شود برای کمک به مدیریت مخاطرات مربوط به زنجیره تأمین ICT در سراسر چرخه حیات محصولات و خدمات، کارفرمایان و تأمین‌کنندگان یک قابلیت سازمانی برای مدیریت زوایای امنیت اطلاعات روابط تأمین‌کننده ایجاد کنند. بهتر است این قابلیت اهداف امنیتی زنجیره تأمین ICT برای سازمان کارفرما را ایجاد و پایش کند و دستاوردهای این اهداف که حداقل شامل موارد زیر هستند را پایش کنند.

الف) تعریف، انتخاب و پیاده‌سازی راهبرد مدیریت مخاطرات امنیت اطلاعات ایجادشده به وسیله آسیب‌پذیری‌های زنجیره تأمین ICT:

1- Data leakage,

۱) برنامه‌ای برای شناسایی آسیب‌پذیری‌های بالقوه مربوط به زنجیره تأمین ICT پیش از آن‌که آسیب‌پذیری‌های بیان‌شده مورد سوءاستفاده قرار گیرند ایجاد شود؛ علاوه بر آن، برنامه‌ای برای کاهش تأثیرات منفی وجود داشته باشد.

۲) مخاطرات مربوط به تهدیدات، آسیب‌پذیری‌ها و عواقب زنجیره تأمین ICT شناسایی و مستندسازی شود (به بند ۶-۳-۴ مراجعه شود)

ب) ایجاد و وفاداری به کنترل‌های پایه امنیت اطلاعات به‌عنوان پیش‌نیاز یک رابطه توانمند تأمین‌کننده (برای ملاحظه نگاشت بند ۶ به استاندارد ۲۷۰۰۲، پیوست ب مراجعه شود)

پ) ایجاد و وفاداری به سامانه‌های پایه و فرایندهای چرخه حیات نرم‌افزار و روش‌های اجرایی ایجاد روابط توانمند تأمین‌کننده با توجه به ملاحظات مدیریت مخاطرات امنیت اطلاعات زنجیره تأمین ICT. (به بند ۶ مراجعه شود).

ت) دارا بودن مجموعه‌ای از الزامات امنیت اطلاعات پایه که برای تمام روابط تأمین‌کننده صادق باشند و سفارشی کردن آن‌ها برای یک تأمین‌کننده خاص، در هنگام نیاز.

ج)ایجاد یک فرایند تکرارپذیر و آزمون‌پذیر برای ایجاد الزامات امنیت اطلاعات مربوط به روابط تأمین‌کننده جدید، مدیریت روابط تأمین‌کننده موجود، درستی‌سنجی و اعتبارسنجی انطباق تأمین‌کنندگان با الزامات امنیت اطلاعات کارفرما و اتمام روابط تأمین‌کننده.

چ) ایجاد فرایندهای مدیریت تغییر برای اطمینان از این‌که تغییراتی که ممکن است بر روی امنیت اطلاعات تأثیر بگذارند در مدت‌زمان مناسب تأیید و به کار بسته شده‌اند.

خ) تعریف روش‌هایی برای شناسایی و مدیریت وقایع مرتبط با زنجیره تأمین ICT یا وقایعی که توسط این زنجیره ایجاد شده‌اند و روش‌هایی برای اشتراک اطلاعات درباره وقایع مربوط به کارفرما و تأمین‌کننده.

۵-۵ فرایندهای چرخه حیات سامانه

فرایندهای چرخه حیات می‌توانند برای تنظیم انتظارات میان کارفرمایان و تأمین‌کنندگان به‌منظور دقت و پاسخگویی در زمینه امنیت اطلاعات کمک کنند. کارفرمایان می‌توانند به‌منظور افزایش دقت آنچه با آن روابط تأمین‌کننده را ایجاد و مدیریت می‌کنند، فرایندهای چرخه حیات را به صورت داخلی پیاده‌سازی کنند. تأمین‌کنندگان می‌توانند فرایندهای چرخه حیات را برای کمک به نمایش دقتی که تأمین‌کنندگان در فرایندهای نرم‌افزار و سامانه با توجه به رابطه تأمین‌کننده اعمال می‌کنند، پیاده‌سازی کنند. در حالی که وجود این فرایندها در ابتدا برای رسیدگی به مخاطرات توسط هر دو گروه کارفرمایان و تأمین‌کنندگان کمک‌کننده است، توصیه می‌شود فعالیت‌های امنیتی تکمیلی در رابطه با زنجیره تأمین ICT با این فرایندها یکپارچه شود.

بسیاری از مخاطرات زنجیره تأمین ICT به سامانه‌ها و نرم‌افزارها مربوط می‌شوند. استفاده از یک رویکرد چرخه حیات فراهم‌شده در ISO/IEC 15288 و ISO/IEC 12207 یک راهکار پابرجا برای مدیریت مخاطرات بیان‌شده ارائه می‌دهد. هر دو استاندارد نحوه به‌کارگیری مجموعه‌ای از فرایندهای یکسان در متن خاصی از سامانه یا نرم‌افزار را فراهم می‌کنند. استاندارد ISO/IEC 12207 حالت خاصی از به‌کارگیری استاندارد

ISO/IEC 15288 است. هر دو استاندارد اجازه استفاده از هر چرخه حیات یا مدل چرخه حیات را فراهم کرده و مجموعه‌ای از فرایندها که می‌توانند در هر چرخه حیات یا فازی از چرخه حیات در زمان مناسب استفاده شوند را ارائه می‌کنند. برای مثال، فرایند مدیریت پیکربندی می‌تواند هم در مدت توسعه سامانه یا نرم‌افزار و هم در فازهای عملیات و نگهداشت چرخه حیات استفاده شود. این استاندارد رویکردی مانند دو استاندارد بیان‌شده را در سطح خلاصه به وسیله بیانیه هدف و تجزیه هر فرایند به روش‌های اجرایی مورد پذیرش قرارداده است.

بند ۵-۸ خلاصه‌ای از روش‌های اجرایی امنیتی خاص زنجیره تأمین ICT را ارائه می‌کند. بند ۶ نگاشتی از این فعالیت‌های زنجیره تأمین ICT برای فرایند چرخه حیات ارائه می‌کند. کارفرمایان و تأمین‌کنندگان بهتر است آن دسته از فعالیت‌هایی که به قابلیت‌های رابطه تأمین‌کننده سازمان خود مربوط است را علاوه بر روابط تأمین‌کننده منفرد بر مبنای سطح مخاطرات ایجادشده به وسیله تأمین‌کنندگان یا کارفرمایان که در بند ۵-۱ توضیح داده شده است فراهم می‌کند.

۵-۶ فرایندهای ISMS در ارتباط با فرایندهای چرخه حیات سامانه

ISO/IEC 27001 یک فرایند مبتنی بر مخاطرات برای پیاده‌سازی سامانه مدیریت امنیت اطلاعات (ISMS) در داخل محدوده تعریف‌شده فراهم می‌کند. وجود ISMS در داخل هر دو سازمان کارفرما و تأمین‌کننده به کارفرمایان و تأمین‌کنندگان برای شروع رسیدگی به مخاطرات زنجیره تأمین ICT و درک نیاز برای کنترل‌ها و فرایندهای امنیت اطلاعات ویژه لازم برای رسیدگی به این مخاطرات، کمک خواهد کرد.

یادآوری- این مطلب با این فرض بیان شده است که محدوده ISMS شامل قسمت‌های ویژه‌ای از سازمان که روابط تأمین‌کننده را ایجاد و نگهداشت می‌کنند، می‌شود.

اگر سازمانی مخاطرات ذاتی زنجیره تأمین ICT را تعریف کند، کنترل‌های ویژه‌ای برای کاهش این مخاطرات باید انتخاب شوند و در صورت امکان کنترل‌های اضافی نیز برای اطمینان از این‌که سازمان تمام این مخاطرات را پوشش داده است، باید انجام شوند. بند ۵-۵ استفاده از این کنترل‌های امنیت اطلاعات را پوشش می‌دهد. پیوست ب کنترل‌های امنیت اطلاعات خاص را به فرایندهای چرخه حیات منفرد در بند ۶ نگاشت می‌کند.

تأمین‌کنندگان می‌توانند با نمایش انطباق با ISO/IEC 27001 رعایت سطح خاصی از دقت را به کارفرما نشان دهند.

زمانی که کارفرمایان و تأمین‌کنندگان ISMS را با توجه به ISO/IEC 27001 ایجاد می‌کنند، بهتر است اطلاعات ایجادشده برای تبادل وضعیت مدیریت امنیت اطلاعات میان کارفرما و تأمین‌کننده استفاده شود. این اطلاعات شامل موارد زیر است:

الف) محدوده ISMS

ب) بیانیه کاربست‌پذیری

پ) برنامه ممیزی

ت) برنامه‌های آگاه‌سازی

ث) مدیریت وقایع

ج) برنامه‌های سنجش

چ) طرح رده‌بندی اطلاعات

ح) مدیریت تغییرات

خ) دیگر کنترل‌های خاص اعمال‌شده مرتبط

۵-۷ کنترل‌های امنیت اطلاعات ISMS در رابطه با امنیت زنجیره تأمین ICT

استاندارد ISO/IEC 27002 شامل تعدادی از کنترل‌هاست که هدف آن‌ها مشخصاً اشخاص[1] خارجی شامل تأمین‌کنندگان هستند. بند ۱۵ استاندارد ISO/IEC 27002 راهنمای ویژه‌ای را برای روابط تأمین‌کننده فراهم می‌کند. این کنترل‌های گسترش‌یافته تکمیلی می‌توانند برای کمک به اعتبارسنجی روش‌های اجرایی تأمین‌کننده برای تضمین امنیت اطلاعات و سامانه‌های اطلاعاتی کارفرما در زمینه فرایندهای چرخه حیات توسط کارفرما به کار گرفته شوند.

پیوست ب کنترل‌های خاص استاندارد ISO/IEC 27002 را برای فرایندهای چرخه حیات منفرد نگاشت می‌کند.

۵-۸ روش‌های اجرایی امنیتی لازم برای زنجیره تأمین ICT

برخی از مخاطرات زنجیره تأمین ICT با به‌کارگیری استانداردهایی که فرایندهای چرخه حیات (ISO/IEC 15288 و ISO/IEC 12207)، الزامات و ساختارهای ISMS(ISO/IEC 27001) و کنترل‌های امنیت اطلاعات (استاندارد ISO/IEC 27002) را فراهم می‌کنند، پوشش داده می‌شوند. روش‌های اجرایی جزئی‌تر مانند موارد زیر برای پوشش کامل این مخاطرات موردنیاز است.

الف) زنجیره حفاظت: کارفرما و تأمین‌کننده اطمینان دارند که هر تغییر و تبادلی در طول چرخه حیات عنصر مجاز، شفاف و قابل درستی‌سنجی است.

ب) دسترسی ویژه حداقلی: کارکنان تنها در سطح اختیار لازم برای انجام مشاغل خود می‌توانند به اطلاعات و سامانه‌های اطلاعاتی حیاتی دسترسی داشته باشند.

پ) جداسازی وظایف: کنترل فرایند ایجاد، تغییر، یا حذف داده‌ها یا فرایندهای توسعه، عملیات، یا حذف سخت‌افزار و نرم‌افزار با اطمینان از این‌که هیچ فرد یا نقشی به‌تنهایی نمی‌تواند یک وظیفه را تکمیل کند.

ت) مقاومت در برابر دستکاری و جمع‌آوری شواهد آن‌ها: تلاش‌هایی که در راستای دستکاری انجام می‌شوند باید مسدود شوند. در صورت رخ دادن دستکاری باید دستکاری‌های بیان‌شده آشکار و قابل بازگشت باشند.

ث) محافظت از پایداری: داده‌ها و اطلاعات حیاتی باید به صورتی مورد محافظت قرار گیرند که حتی در صورت انتقال اطلاعات یا داده‌های موردنظر از محل ایجاد یا تغییر اولیه خود، همچنان کارا باقی بمانند.

ج)مدیریت انطباق: موفقیت محافظت در محدوده توافقنامه می‌تواند به صورت مستمر و مستقل تأیید شود.

1- Parties

چ) ارزیابی و درستی‌سنجی کد: روش‌هایی برای بازرسی کد به کار گرفته شده و کدهای مشکوک شناسایی می‌شوند.

ح) آموزش امنیت زنجیره تأمین ICT: توانایی سازمان در آموزش کارآمد کارکنان مرتبط در مورد روش‌های اجرایی امنیت اطلاعات. توصیه می‌شود این روش‌های اجرایی شامل روش‌های اجرایی توسعه امن، تشخیص ایجاد تداخل و غیره در زمان مناسب باشند.

خ) ارزیابی و پاسخگویی در مورد آسیب‌پذیری: درک رسمی از سوی کارفرما درباره این‌که وضعیت تجهیز تأمین‌کنندگان با قابلیت جمع‌آوری ورودی‌هایی درباره آسیب‌پذیری‌ها از محققین، مشتریان یا منابع و به‌منظور ایجاد یک تحلیل تأثیر معنی‌دار و راه‌حل‌های مناسب در زمان کوتاه تا چه اندازه مناسب است، انجام می‌پذیرد. این ارزیابی باید شامل توافق کارفرما و تأمین‌کننده بر روی فرایندهای تکرارپذیر پاسخگویی به آسیب‌پذیری‌ها باشد.

د) انتظارات تعریف‌شده: الزاماتی که باید به وسیله عناصر و محیط طراحی/توسعه رعایت شوند پیشاپیش در توافقنامه با زبان شفاف بیان می‌شوند. توصیه می‌شود این انتظارات شامل تعهد به تأمین آزمون امنیت اطلاعات، رفع مشکلات کد و تضمین‌هایی در رابطه با توسعه، یکپارچه‌سازی و فرایندهای تحویل استفاده شده باشند.

ذ) مالکیت و مسئولیت‌ها: مالکیت حقوق معنوی توسط کارفرما و تأمین‌کننده و مسئولیت دیگر اشخاص در مورد محافظت از حقوق معنوی در توافقنامه شناسایی می‌شوند.

ر) اجتناب از مؤلفه‌های بازار خاکستری[1]: به وسیله الزام درستی‌سنجی هویت مؤلفه‌های سامانه می‌توان از بسیاری از مخاطرات زنجیره تأمین ICT اجتناب نمود.

ز) اکتساب ناشناس[2]: هنگامی‌که مناسب و امکان‌پذیر باشد، از اکتساب بی‌نام استفاده شود؛ زمانی که هویت کارفرما حساس است، ارتباط زنجیره تأمین فناوری اطلاعات و کارفرما مسدود شود.

ژ) اکتساب یک‌جا[3]: ممکن است مؤلفه‌های سامانه‌های طولانی‌مدت(کنترل‌های خودکار مانا) قدیمی شوند و مخاطرات زنجیره امنیت ICT را افزایش دهند، اکتساب تمام بخش‌های پراکنده در یک قالب زمانی مشخص این مخاطرات را کاهش می‌دهد.

س) الزامات بازگشتی برای تأمین‌کننده: قراردادها می‌توانند تعیین کنند که تأمین‌کنندگان الزامات زنجیره تأمین ICT را برای تأمین‌کنندگان بالادست خود مقرر و اعتبارسنجی کرده‌اند.

۶ امنیت زنجیره تأمین ICT در فرایندهای چرخه حیات

۶-۱ فرایندهای توافق

روابط تأمین‌کننده بین کارفرمایان و تأمین‌کنندگان به وسیله توافقات حاصل می‌شود. سازمان‌ها می‌توانند به صورت همزمان یا سلسله‌ای به‌عنوان کارفرما و تأمین‌کننده محصولات و خدمات ICT ایفای نقش کنند. برای

1- Gray-market
2- Anonymous acquisition
3- All-at-once acquisition

موارد خاصی که کارفرما و تأمین‌کننده عضو یک سازمان واحد هستند، توصیه می‌شود که همچنان از فرایندهای توافق استفاده شود اما این فرایند دارای رسمیت کمتری باشد. فرایندهای توافق شامل فرایند اکتساب و فرایند تأمین است.

استاندارد ISO/IEC 27002 راهنمای تکمیلی مشخصی را درباره انتظارات از تنظیمات در طول فرایندهای توافق فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آورده شده است.

۶-۱-۱ فرایندهای اکتساب

هدف یک فرایند اکتساب، تهیه محصول یا انجام خدمت مطابق با الزامات کارفرما است.[1] استاندارد ISO/IEC 15288 راهنمایی درباره پیاده‌سازی یک فرایند اکتساب فراهم می‌کند. کارفرمایان بهتر است فعالیت‌های زیر را به‌عنوان قسمتی از فرایند اکتساب به‌منظور اطمینان از این‌که آن‌ها مخاطرات زنجیره تأمین ICT را به صورت مناسب مدیریت می‌کنند انجام دهند:

الف) آمادگی برای اکتساب.

۱) راهبردی برای چگونگی انجام اکتساب ایجاد شود.

- راهبردهای تأمین منبع بر مبنای تحمل مخاطرات امنیت اطلاعات در مورد مخاطرات زنجیره تأمین ICT ایجاد شود.
- مشخص کردن مجموعه‌ای از الزامات امنیت اطلاعات پایه که در مورد تمام روابط با تأمین‌کننده صادق هستند.

۲) مجموعه الزامات پایه امنیت اطلاعات برای روابط خاص با تأمین‌کنندگان به‌منظور آماده‌سازی تقاضایی برای تأمین محصول یا خدمتی که تعریف زیر از الزامات در بر می‌گیرد متناسب‌سازی شود.

- ایجاد الزامات امنیت اطلاعات برای تأمین‌کنندگان شامل الزامات مقرراتی[2] مربوط به ICT (یعنی مخابرات و فناوری اطلاعات)، الزامات فنی، زنجیره حفاظت، شفافیت و مشاهده‌پذیری، اشتراک اطلاعات درباره وقایع امنیت اطلاعات در سراسر زنجیره تأمین، قواعدی[3] برای از رده خارج کردن یا نگهداری عناصری مانند مؤلفه‌ها، داده یا دارایی معنوی و دیگر الزامات مرتبط.
- ایجاد الزاماتی برای مدیریت تأمین‌کنندگان در زنجیره تأمین ICT در مواقع مناسب.
- تعریف الزاماتی برای فراهم کردن شواهد معتبری به‌منظور نمایش برآورده کردن الزامات امنیت اطلاعات توسط تأمین‌کنندگان زنجیره تأمین ICT.
- تعریف الزاماتی برای تأمین‌کنندگان عناصر حیاتی در زنجیره تأمین ICT که نمایش قابلیتی برای اصلاح آسیب‌پذیری‌های پدیدارشونده را بر مبنای اطلاعات جمع‌آوری‌شده از کارفرما و دیگر منابع برای پاسخگویی به وقایع و اصلاح آسیب‌پذیری‌هایی که به واقعه موردنظر ختم شده‌اند را الزام کنند.

1- ISO/IEC 15288, Systems and software engineering — System life cycle processes
2- Regulatory requirements
3- Rules

- شناسایی الزاماتی برای مالکیت دارایی‌های فکری و مسئولیت‌های کارفرما و تأمین‌کننده برای عناصری مانند کد نرم‌افزار، داده و اطلاعات، محیط تولید/ توسعه/یکپارچه‌سازی، طراحی و فرایندهای اختصاصی.
تعریف الزاماتی برای شناسایی دوره حیات مورد انتظار عناصر توسط تأمین‌کننده تا به کارفرما برای برنامه‌ریزی در مورد هر نوع مهاجرتی که ممکن است برای پشتیبانی از سامانه مستمر و عملیات در راستای مأموریت لازم است، کمک کند.
تعریف الزاماتی برای ممیزی سامانه‌های اطلاعات تأمین‌کننده در جایی که قابل‌کاربرد است.
تعریف الزاماتی برای پایش فرایندهای کاری تأمین‌کنندگان و محصولات کاری در جایی که قابل‌کاربردست.
به اشتراک گذاشتن الزامات کارفرما در سراسر زنجیره تأمین اطلاعات، تعریف الزامات برای ارتباط با آن‌ها و الزام کردن آن‌ها برای تأمین‌کنندگان بالادست.
ب) تبلیغ اکتساب و انتخاب تأمین‌کننده.
۱) ارسال درخواست تأمین محصول یا خدمت موردنظر را برای تأمین‌کنندگان شناخته‌شده
- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.
۲) انتخاب یک یا چند تأمین‌کننده
- انتخاب تأمین‌کنندگان بر مبنای ارزیابی توانایی آن‌ها در برآورده کردن الزامات مشخص شامل الزامات موجود در زنجیره تأمین ICT
- استفاده از روش‌ها و نتایج ارزیابی پابرجا برای محصولات، خدمات، مؤلفه‌های ICT یا تأمین‌کنندگان آن‌ها (مانند مخازن ISO/IEC 15408 برای مؤلفه‌ها یا گواهی سامانه مدیریت امنیت اطلاعات (ISMS) برای تأمین‌کنندگان) به‌عنوان معیارهایی برای ارزیابی انطباق با الزامات مشخص‌شده.
- به‌کارگیری ملاحظات مربوط به سوابق کارهای گذشته تأمین‌کنندگان در مورد خط‌مشی‌های[1] کارکنان، روش‌های اجرایی، و روال‌های امنیت اطلاعات به‌عنوان قسمتی از فرایندها و الزامات انتخاب منبع
پ) آغاز توافق
۱) مذاکره درباره توافق با تأمین‌کننده.
مذاکره درباره توافق با تأمین‌کننده یا تأمین‌کنندگان منتخب و تصریح الزامات توافق‌شده قابل کاربرد در زنجیره تأمین ICT در توافقنامه.
۲) آغاز توافق با تأمین‌کننده.
- ایجاد و نگهداشت برنامه‌ای برای اطمینان از یکپارچگی محصولات نرم‌افزاری و سخت‌افزاری موجود و مؤلفه‌های فراهم‌شده از طریق زنجیره تأمین ICT.
ت) پایش توافق.
۱) ارزیابی و اجرای توافقنامه.
- ایجاد و نگهداشت رویه و معیارهای درستی‌سنجی محصولات و خدمات تحویل‌شده.
- ممیزی سامانه‌های اطلاعاتی تأمین‌کنندگان در موارد قابل‌کاربرد.

1- Policy

- پایش و ارزیابی فرایندهای تأمین‌کننده (مانند طراحی، روش‌های اجرایی تحویل و غیره) و محصولات کاری در موارد قابل‌کاربرد.

۲) تأمین داده‌های لازم توسط تأمین‌کننده و حل مسائل در زمان معقول.

- گزارش ضعف‌ها و آسیب‌پذیری‌های امنیت اطلاعاتی که در استفاده از محصولات و خدمات ICT فراهم‌شده از طریق زنجیره تأمین شناسایی شده‌اند.

۳) ارزیابی تأمین‌کنندگان برای توانایی آن‌ها در برآورده‌کردن الزامات مشخص‌شده زنجیره تأمین ICT

ث) پذیرش محصول یا خدمت

۱) تأیید این‌که محصول یا خدمت تحویل‌شده یا توافق صورت‌گرفته مطابقت دارد.

- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.

۲) انجام پرداخت یا فراهم کردن موارد توافق‌شده دیگر برای تأمین‌کننده برای محصولات و خدمات تحویل‌شده که برای بستن توافق لازم است.

- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.

۶-۱-۲ فرایند توافق

هدف فرایند توافق، فراهم کردن محصولات و خدمات منطبق بر الزامات توافقنامه برای کارفرما است[1]. توصیه می‌شود تأمین‌کنندگان زنجیره تأمین ICT فعالیت‌های زیر را به‌عنوان قسمتی از فرایند تأمین به‌منظور تضمین و نمایش این‌که مخاطرات زنجیره تأمین ICT را به شکل مناسب مدیریت می‌کنند در نظر بگیرند.

الف) شناسایی فرصت‌ها

۱) تعیین وجود و هویت کارفرمایی که نماینده سازمان یا سازمان‌هایی است که به محصول یا خدمتی احتیاج دارند.

- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.

ب) پاسخ به مناقصه

۱) ارزیابی تقاضا برای تأمین محصول یا خدمت به‌منظور تعیین امکان‌پذیری و چگونگی پاسخ به مناقصه.

- مشخص کردن مجموعه‌ای از الزامات امنیت اطلاعات پایه که برای تمام روابط با تأمین‌کنندگان صادق است به همراه متناسب‌سازی در مواقع موردنیاز.

۲) آماده کردن پاسخی که درخواست موردنظر را برآورده کند.

- ایجاد راهی برای نمایش توانایی تحویل محصولات و خدماتی که به الزامات امنیت اطلاعات کارفرما شامل الزامات قانون‌گذاری[2] مربوط به ICT (یعنی مخابرات و فناوری اطلاعات)، الزامات فنی، زنجیره حفاظت، شفافیت و مشاهده‌پذیری، اشتراک اطلاعات در مورد وقایع امنیت اطلاعات در سراسر زنجیره تأمین، قواعدی برای از رده خارج کردن یا حفظ عناصری مانند مؤلفه‌ها، داده، یا دارایی معنوی و دیگر الزامات مرتبط.

1- ISO/IEC 15288

2- Requlatory requirements

- متناسب‌سازی مجموعه‌ای از الزامات پایه امنیت اطلاعات برای روابط تأمین‌کننده خاص با تأمین‌کننده در مواقع نیاز.
- مشخص کردن الزاماتی برای فراهم کردن شواهد معتبر در مورد رعایت الزامات کارفرما.
پ) آغاز یک توافق.
۱) مذاکره در مورد توافق با کارفرما.
- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.
۲) آغاز توافق با کارفرما.
- ایجاد و نگهداشت برنامه‌ای برای تضمین یکپارچگی محصولات و مؤلفه‌های نرم‌افزاری و سخت‌افزاری تحویل‌شده.
- ایجاد و نگهداشت برنامه‌ای برای تضمین حفاظت از حقوق مالکیت معنوی مانند آن دست از آن‌ها که مربوط به داده و اطلاعات، طراحی، فرایندها، محیط و غیره هستند.
ت)اجرای توافقنامه
۱) اجرای توافقنامه با توجه به برنامه‌های مدیریت پروژه ایجادشده توسط تأمین‌کننده در رابطه با توافق.
- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.
۲) ارزیابی اجرای توافقنامه
- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.
ث) تحویل و پشتیبانی محصول یا خدمت.
۱) تحویل محصول یا خدمت با توجه به معیارهای توافقنامه.
- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.
۲) فراهم کردن کمک‌های لازم به تأمین‌کننده در راستای پشتیبانی از سامانه یا خدمت تحویل‌شده با توجه به معیارهای توافقنامه.
- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.
ج) بستن توافقنامه.
۱) پذیرش و تأیید پرداخت یا موارد توافق‌شده دیگر.
- هیچ فعالیتی که مختص زنجیره تأمین ICT باشد موردنیاز نیست.
۲) انتقال مسئولیت محصول یا خدمت به کارفرما یا شخص دیگر برای بستن توافق به نحوی که در توافقنامه مشخص شده است
۳) تضمین اجرا نگهداری سنجه‌های امنیتی توافق‌شده در پایان مدت توافقنامه.

۲-۶ فرایندهای توانمندساز پروژه سازمانی

فرایندهای توانمندساز پروژه سازمانی در ارتباط با تضمین این‌که منابع موردنیاز برای توانمند کردن پروژه در راستای برآورده‌کردن نیازها و انتظارات اشخاص ذینفع سازمان فراهم شده‌اند، است.

فرایندهای توانمندساز پروژه سازمانی محیطی را که پروژه‌ها در آن‌ها انجام می‌شوند را ایجاد می‌کند[1]. این فرایندها مگر در زمانی که صریحاً خلاف آن بیان شده باشد، برای هر دو طرف کارفرما و تأمین‌کننده قابل به‌کارگیری هستند.

استاندارد ISO/IEC 27002 راهنماهای مشخص تکمیلی را در رابطه تنظیم انتظارات در طول فرایندهای توانمندساز پروژه سازمانی فراهم می‌کنند. نگاشت بند ۶ قسمت ۳ استاندارد ISO/IEC 27036 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب فراهم شده است.

۶-۲-۱ فرایند مدیریت مدل چرخه حیات

هدف فرایند مدیریت مدل چرخه حیات تعریف، نگهداشت، و تضمین دسترس‌پذیری خط‌مشی‌ها، فرایندهای چرخه حیات، مدل‌ها و رویه‌هایی چرخه حیات برای استفاده توسط سازمان است[2]. توصیه می‌شود امنیت زنجیره تأمین ICT در این فرایند مدنظر قرار گیرد، اما هیچ راهنمای مشخصی علاوه بر استانداردهای ISO/IEC 15288 و ISO/IEC 27036-2 در این زمینه وجود ندارد.

۶-۲-۲ فرایند مدیریت زیرساخت

هدف فرایند مدیریت زیرساخت فراهم کردن زیرساخت توانمند ساز زنجیره تأمین ICT در راستای پشتیبانی کارفرمایان و تأمین‌کنندگان در سراسر زنجیره است.

یادآوری- استاندارد ISO/IEC 15288 هدف فرایند مدیریت زیرساخت را به‌صورت زیر تعریف می‌کند:

هدف فرایند مدیریت زیرساخت فراهم کردن زیرساخت و خدمات توانمند ساز برای پروژه‌ها در راستای پشتیبانی سازمان‌ها و اهداف پروژه در سراسر زنجیره است.

توصیه می‌شود کارفرمایان و تأمین‌کنندگان موارد زیر را در جایی که قابل‌کاربرد هستند در راستای رسیدگی به مخاطرات امنیت اطلاعات در زنجیره تأمین ICT به‌عنوان قسمتی از فرایند مدیریت زیرساخت در نظر گیرند:

الف) ایجاد و نگهداشت مشاهده‌پذیری فرایندها، محیط و دارایی‌های مرتبط دیگر برای تولید یا عملیاتی کردن محصولات یا خدمات.

ب) ایجاد و نگهداشت مشاهده‌پذیری محیط‌های توسعه، یکپارچه‌سازی و تولید شامل داشتن موجودی دارایی‌ها در محیط.

پ) ایجاد فرایندها و قابلیت‌های امنیت فیزیکی برای مؤلفه‌های امنیتی و رسانه‌ها شامل حذف و نگهداشت در زمان تحویل.

ت) ایجاد امنیت مخزن کد شامل میزبانی تمام دارایی‌های مربوط به کد در مخازن کد منبع امن با دسترسی ممیزی‌شده و کنترل‌شده.

ج) ایجاد امنیت محیط طراحی/ توسعه شامل محیط‌های ساخت خودکار با مالکان کم و ردیابی بالای

1- ISO/IEC 15288
2- ISO/IEC 15288

عملکردها در ساخت نبشته‌ها[1] و دسترسی به پرونده‌های کد در زمان ساخت و همچنین محافظت یکسان از برای ساخت نبشته‌ها به اندازه یکسان با دیگر دارایی‌های کد (شامل ورود آن‌ها به مخزن کد).

چ) ایجاد یک برنامه اسکن بدافزارها برای کدهای تحت توسعه و همچنین محیط توسعه، حداقل تا سطحی که در استاندارد ISO/IEC 27002 توضیح داده شده است.

ح) پیاده‌سازی فرایندهای تبادل کدی که یکپارچگی و اصالت را به کمک بسته‌های دارای امضای دیجیتال، جمع‌آزما[2] و تابع چکیده‌ساز تضمین کند.

خ) پیاده‌سازی روش‌های مشهودسازی دست‌کاری‌ها و بسته‌بندی آن‌ها برای تحویل اقلام فیزیکی.

یادآوری- این فرایند تسهیلات، ابزارها، ارتباطات و دارایی‌های فناوری اطلاعاتی که برای کسب‌وکار سازمان با توجه به محدوده این استاندارد ملی لازم است را تعریف، فراهم و نگهداری می‌کند.

[ISO/IEC 15288]

۶-۲-۳ فرایند مدیریت سبد[3] پروژه

هدف از فرایند مدیریت سبد پروژه آغاز و نگهداری پروژه‌های لازم، کافی و مناسب برای پروژه در راستای برآورده‌کردن اهداف راهبردی سازمان است[4]. توصیه می‌شود کارفرمایان و تأمین‌کنندگان فرایندهای زنجیره تأمین ICT را مدنظر قرار دهند اما هیچ راهنمای مشخصی علاوه بر ISO/IEC 15288 و ISO/IEC 27036-2 در این زمینه وجود ندارد.

۶-۲-۴ فرایند مدیریت منابع انسانی

هدف از فرایند مدیریت منابع انسانی تضمین این است که منابع انسانی لازم برای سازمان فراهم شده و صلاحیت آن‌ها مطابق با نیازهای سازمان نگه‌داشته می‌شود[5]. علاوه بر آن، برای پیاده‌سازی فرایند مدیریت منابع انسانی در ISO/IEC 15288 و کنترل‌های امنیتی منابع انسانی در استاندارد ISO/IEC 27002، توصیه می‌شود کارفرمایان و تأمین‌کنندگان نیروهایی را درباره مسائل ویژه زنجیره تأمین ICT و چگونگی رسیدگی به آن‌ها آموزش دهند. مشخصاً، توصیه می‌شود کارفرمایان و تأمین‌کنندگان کارهای زیر را با در نظر گرفتن الزاماتی که میان کارفرما و تأمین‌کننده در زنجیره تأمین ICT به اشتراک گذاشته خواهند شد انجام دهند.

الف) ایجاد سیاست سازمانی و الزامات قراردادی عمومی را به‌منظور آگاه‌سازی و آموزش در زمینه مدیریت مخاطرات زنجیره تأمین ICT.

ب) تعریف و الزام نقش‌ها را در سراسر زنجیره تأمین ICT چرخه حیات عنصر/سامانه به‌منظور محدود کردن فرصت‌ها و ابزاری که در اختیار افراد انجام‌دهنده این نقش‌ها بوده و می‌تواند موجب عواقب نامطلوب شود.

پ) توسعه یک برنامه جامع برای آگاه‌سازی و آموزش که خط‌مشی‌ها و روش‌های اجرایی امنیت زنجیره

1- Scripts
2- Checksum
3- Portfolio
4- ISO/IEC 15288
5- Comperencies

تأمین ICT سازمان را ترویج کند.

ت) آموزش کارکنان تضمین کیفیت و امنیت اطلاعات در مورد روشگان‌های ارزیابی تهدیدات و آسیب‌پذیری‌های زنجیره تأمین ICT.

ث) آموزش کارکنان دریافت‌کننده (مانند کارکنان فنی، متخصصین تجهیزات و مدیران آیتم (قلم)) درباره فرایند صحیح دریافت عناصر/ خدمات (شامل قسمت‌های پراکنده)، شامل هر ناهنجاری شناخته‌شده مربوط به قسمت‌ها (که ممکن است بیانگر جعل، خرابکاری و مشکلات کیفی باشد)

ج) آموزش توسعه‌دهندگان نرم‌افزار در مورد روش‌های اجرایی کدنویسی امن و اهمیت آن برای رفع مخاطرات امنیت اطلاعات مربوط به مخاطرات زنجیره تأمین ICT و کاهش تعداد آسیب‌پذیری‌ها در کد تحویل‌شده.

چ) ایجاد و اجرای الزامات مربوط به ارزیابی و بازنگری امنیت کارکنان. این بازنگری‌ها و ارزیابی‌ها باید شامل افرادی شود که به عناصر، فرایندهای عناصر، یا فعالیت‌های کسب‌وکاری که فرصت به‌کارگیری دانش فنی یا درک فرایندهای کسب‌وکار را برای به دست آوردن دسترسی غیرمجاز به عناصر یا فرایندهایی که می‌توانند به تسخیر یا فقدان ختم شوند، دسترسی دارند.

ح) تعریف فرایندهایی برای جمع‌آوری اطلاعات عمومی درباره زنجیره تأمین ICT، استخراج درس‌های آموخته‌شده، و اشتراک آن‌ها میان کارکنان کارفرمایان و تأمین‌کنندگان به نحوی که در محدوده قرارداد مشخص شده است.

خ) پیاده‌سازی مدیریت هویت، کنترل‌های دسترسی، و پایش فرایند به‌منظور فراهم کردن امکان کشف و طبقه‌بندی رفتارها یا کارکنان ناهنجار که می‌تواند به عواقب نامطلوب در مورد دسترسی فیزیکی یا منطقی در زنجیره تأمین ICT ختم شود.

د) ایجاد و اجرای الزامات انتساب شناسه‌های منحصر به فرد به افراد (مانند حساب ورود به سامانه، شناسه کاربری و غیره) شامل الزاماتی که شرایط استفاده مجدد از چنین اقلامی را مشخص می‌نمایند (مانند اخراج کارکنان، تغییر نام و غیره)

۶-۲-۵ فرایند مدیریت کیفیت

هدف از فرایند مدیریت کیفیت اطمینان از این موضوع است که محصولات، خدمات و پیاده‌سازی‌های فرایندهای چرخه حیات یک زنجیره تأمین ICT اهداف مدیریت کیفیت سازمان را برآورده کرده و رضایت مشتری را تأمین می‌نمایند.

یادآوری ۱- استاندارد ISO/IEC 15288 هدف فرایند مدیریت کیفیت را به شکل زیر بیان می‌کند.

هدف از فرایند مدیریت کیفیت، اطمینان از این موضوع است که محصولات، خدمات و پیاده‌سازی چرخه حیات فرایندها اهداف کیفیتی سازمان را برآورده کرده و رضایت مشتری را تأمین می‌کند.

کارفرمایان و تأمین‌کنندگان باید موارد زیر را به‌عنوان قسمتی از فرایند مدیریت کیفیت خود برای رفع

مخاطرات امنیتی اطلاعات در زنجیره تأمین بگنجانند.

الف) برنامه مدیریت فعال آسیب‌پذیری در پایین‌ترین سطح در مقایسه با آنچه در استاندارد ISO/IEC 27002 شرح داده شده است.

یادآوری ۲- فعالیت‌های عمومی مدیریت آسیب‌پذیری تحت فرایند مدیریت مخاطرات بند ۶-۳-۴پوشش داده شده‌اند.

ب) یکپارچه‌سازی آزمون‌های مربوط به ضعف‌ها و آسیب‌پذیری‌ها با فعالیت‌های مدیریت کیفیت از طریق چرخه حیات توسعه سامانه شامل بازنگری طراحی و معماری، بازنگری‌های مستند و انواع آزمون‌هایی که نرم‌افزار و سخت‌افزار پیش از تحویل و نصب و در هنگام به‌روزرسانی پشت سر می‌گذارند.

یادآوری ۳- یکپارچه‌سازی آزمون‌های اطمینان‌پذیری و مقاومت با فعالیت‌های مدیریت کیفیت بهتر است به شکل مناسب مدنظر قرار گیرند.

۶-۳ فرایندهای پروژه

فرایندهای پروژه در رابطه با مدیریت پروژه دقیق و پشتیبانی پروژه برای پروژه‌های مهندسی سامانه و نرم‌افزار، شامل فرایندهایی که در زنجیره یا زنجیره‌های تأمین ICT شکسته می‌شوند، است. این فرایندها هم برای کارفرمایان و هم برای تأمین‌کنندگان صادق هستند، مگر درصورتی‌که مشخصاً خلاف آن بیان شود.

۶-۳-۱ فرایند طرح‌ریزی پروژه

هدف از فرایند برنامه‌ریزی پروژه تولید و ارتباط مؤثر و کارآمد برنامه‌های پروژه است[1]. برای پروژه‌هایی که محصولات و خدمات ایجادشده و تحویل‌شده در زنجیره‌های تأمین پراکنده از نظر جغرافیایی که توسط چندین هستار، کارفرما و تأمین‌کننده کنترل می‌شوند توصیه می‌شود که در طول فرایند برنامه‌ریزی پروژه موارد زیر را در نظر گرفته و یکپارچه کنند:

الف) چگونگی تأثیر نیاز به ایمن‌سازی اطلاعات کارفرما و تأمین‌کننده بر روی برنامه‌ها زمان‌بندی‌های پروژه.

ب) هر جنبه‌ای از مدیریت مخاطرات امنیت اطلاعات زنجیره تأمین ICT که باید در نقش‌ها، مسئولیت‌ها، پاسخگویی‌ها و اختیارات پروژه لحاظ شود.

پ) الزامات قانونی[2] مختلف حوزه‌های قضایی[3] چندگانه مرتبط با زنجیره تأمین ICT.

ت) منابعی که برای تضمین حفاظت از اطلاعات کارفرما و تأمین‌کننده شامل الزامات تأمین نیرو در طول زنجیره(ها)ی تأمین ICT لازم هستند.

۶-۳-۲ فرایند ارزیابی و کنترل پروژه

هدف از فرایند ارزیابی و کنترل پروژه، تعیین وضعیت پروژه و اجرای مستقیم برنامه پروژه برای تضمین این‌که پروژه در راستای برنامه و زمان‌بندی، در محدوده بودجه مقرر و در جهت برآورده‌کردن اهداف فنی

1- ISO/IEC 15288
2- Legal requirements
3- jurisdiction

حرکت می‌کند است. علاوه بر پیاده‌سازی فرایند ارزیابی و کنترل پروژه در ISO/IEC 15288 و ISO/IEC 27036-2 توصیه می‌شود، کارفرمایان موارد زیر را پیاده‌سازی کنند:

الف) انجام ممیزی انطباق دوره‌ای محصولات یا خدمات تأمین‌کننده به‌منظور تعیین این‌که تأمین‌کنندگان همچنان به الزامات کارفرما پایبند هستند یا خیر. مستندسازی نتایج این ممیزی‌ها در گزارش انطباق. بهتر است تناوب ممیزی‌های انطباق بر مبنای مخاطرات امنیتی زنجیره تأمین ICT و تحمل مخاطرات از سوی کارفرما تعیین شوند.

۶-۳-۳ فرایند مدیریت تصمیم

هدف از فرایند مدیریت تصمیم، انتخاب مفیدترین عملیات پروژه در زمانی است که عملیات جایگزین وجود دارد[1]. بهتر است کارفرمایان و تأمین‌کنندگان امنیت زنجیره تأمین ICT در این فرایند را در نظر بگیرند، اما هیچ راهنمای مشخصی علاوه بر ISO/IEC 15288 و ISO/IEC 27036-2 در این زمینه وجود ندارد.

۶-۳-۴ فرایند مدیریت مخاطرات

هدف از فرایند مدیریت مخاطرات، شناسایی، تحلیل، مداوا و پایش مخاطرات به‌صورت مستمر است.[2] علاوه بر پیاده‌سازی فرایند مدیریت مخاطرات در ISO/IEC 15288 و ISO/IEC 27036-2 و رویکرد مدیریت مخاطرات امنیت اطلاعاتی که در ISO/IEC 27005 توضیح داده شده است، کارفرمایان و تأمین‌کنندگان باید فعالیت‌های زیر را به‌منظور پوشش مخاطرات امنیت اطلاعات در زنجیره تأمین ICT انجام دهند:

الف) شناسایی تهدیدات، آسیب‌پذیری‌ها و عواقب مربوط به محصولات و خدمات ICT.

ب) شناسایی و مستندسازی مخاطرات زنجیره تأمین ICT مرتبط با تهدیدات و آسیب‌پذیری‌های شناسایی‌شده.

پ) شناسایی الزامات قانونی[3] حوزه‌های مختلف مرتبط با زنجیره تأمین ICT

ت) تعریف و انتخاب راهبرد مدیریت مخاطرات زنجیره تأمین ICT رخ‌داده به دلیل ضعف‌ها و آسیب‌پذیری‌های غیرعمدی و عمدی.

ث) تعیین محدوده مسئولیت‌های کاهش مخاطرات زنجیره تأمین ICT در میان کارفرمایان و تأمین‌کنندگان.

ج) ایجاد فرایندهای ارتباط مخاطرات در میان کارفرمایان و تأمین‌کنندگان.

چ) شناسایی اثربخشی عملیات اصلاحی گذشته به‌وسیله تأمین‌کنندگان در سراسر زنجیره تأمین در محصولات یا خدمات دیگر که در فعالیت‌های آینده قابل‌کاربرد هستند.

ح) تعیین دلایل ریشه‌ای ضعف‌ها و آسیب‌پذیری‌هایی که در زمان توسعه، تحویل و عملیاتی کردن شناسایی می‌شوند. اقدامات متقابل و کاهش‌ها در مواقع مناسب، پیاده‌سازی شوند.

1- ISO/IEC 15288
2- ISO/IEC 15288
3- Legal requirements

خ) زنجیره تـأمین ICT را بـرای یـافتن مسـائل بـالقوه، شناسـایی و تحلیـل مخـاطرات امنیـت اطلاعـات و به‌روزرسانی راهبردهای ارزیابی و مداوای مخاطرات پایش نمایید.

۶-۳-۵ فرایند مدیریت پیکربندی

هدف از فرایند مدیریت پیکربندی، ایجاد و نگهداری یکپارچگی کلیه خروجی‌های شناخته‌شده یک پروژه یا فرایند و دسترس‌پذیر کردن آن‌ها برای تمامی اشخاص درگیر است[1]. مدیریت پیکربندی برای درک تغییرات انجام‌شده در محصولات، سامانه‌ها، عناصر محصول و سامانه، مستندات مرتبط، و خود زنجیره تأمین شامل افرادی که تغییرات را انجام می‌دهند، حیاتی است. به‌منظور تضمین آن‌که مسائل زنجیره تأمین به صورت مناسب مدیریت‌شده‌اند، توصیه می‌شود کارفرمایان و تأمین‌کنندگان در مواقع مناسب، موارد زیر را به‌عنوان قسمتی از فرایند مدیریت پیکربندی خود در نظر گیرند تا مخاطرات خاص امنیت اطلاعات در زنجیره تأمین ICT مدیریت شوند:

الف) کنترل دسترسی و تغییرات در تمام سخت‌افزارها و عناصر سخت‌افزاری در سراسر چرخه حیات شامل طراحی، تولید، آزمون، عملیات، نگهداری و از رده خارج شدن.

ب) کنترل دسترسی و تغییرات در مستندات مربوط به محصولات و خدمات ICT

پ) تأیید و مدیریت تغییرات در روش‌های تحویل، به دو صورت منطقی و فیزیکی.

ت) تأیید و مدیریت تغییرات در سامانه‌ها و نرم‌افزارها شامل کد منبع، ساختارها و مقادیر پایگاه داده.

ث) گنجاندن تمامی دارایی‌های مرتبط در مخازن کد منبع به‌منظور توانمندسازی توجه بیشتر به امنیت اطلاعات و کنترل دسترسی.

ج) قراردادن تمامی کارسازهایی[2] که میزبانی مخازن کد منبع را بر عهده دارند در محل امن، پیکربندی آن‌ها به شکلی که به‌صورت پیش‌فرض امن باشند (به‌عنوان مثال با اعطای کمترین دسترسی ویژه و غیرفعال کردن خدماتی که به‌صورت گسترده موردنیاز نیستند)، و محافظت مناسب از این کارسازها در مقابل حساسیت کدی که بر روی آن‌ها اجرا می‌شود.

چ) کنترل دسترسی به مخازن کد از طریق استفاده از سامانه‌های هویت شرکتی با کنترل شدیدی که در دسترسی به هر کدام از حساب‌های کاربری سامانه اعمال می‌شود؛ اصل تفکیک وظایف باید مورد ملاحظه قرار گرفته و دسترسی سطح بالا تنها در مواقع لازم اجازه داده شود.

ح) مدیریت اجازه‌های دسترسی به مخازن، شامل دسترسی به شعب، حوزه‌های کاری یا مجموعه‌های کد؛ و اعطای اجازه دسترسی مبتنی بر کمترین اجازه و میزان اطلاعاتی که دانستن آن‌ها لازم است.

خ) محافظت از تغییرات مخازن کد شامل بازنگری و تأیید را برای تحلیل آتی.

د) ثبت اسامی پرونده‌ها، نام حساب کاربری فردی که پرونده را بررسی می‌کند، مهر زمانی ورود[3]، و خطی که در رخدادنگار تغییر[4]، تغییر کرده است.

1- ISO/IEC 15288
2- Servers
3- Check-in Timestamp
4 Change log

ذ) نگهداری و مدیریت بیانیه‌ای از تمامی دارایی‌های کدی که در ایجاد محصول شامل محصولات داخلی و محصولات توسعه‌داده‌شده توسط تأمین‌کننده نقش دارند.

ر) ایجاد و حفاظت از زنجیره محافظت از هر عنصر از طریق امضای کد، مهر زمانی و فنون مناسب دیگر.

استاندارد ISO/IEC 27002راهنمای ویژه تکمیلی درباره تنظیم انتظارات در طی فرایند مدیریت پیکربندی فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۳-۶ فرایند مدیریت اطلاعات

هدف از فرایند مدیریت اطلاعات، فراهم کردن اطلاعات مرتبط، به‌موقع، کامل، معتبر و در صورت لزوم محرمانه برای اشخاص شناسایی‌شده در طول چرخه حیات زنجیره تأمین ICT و حتی در مواقع مناسب پس از اتمام چرخه حیات زنجیره تأمین ICT است.

یادآوری – استاندارد ISO/IEC 15288 هدف از فرایند مدیریت اطلاعات را به شکل زیر بیان می‌کند.

هدف از فرایند مدیریت کیفیت، فراهم کردن اطلاعات مرتبط، به‌موقع، کامل، معتبر و در صورت لزوم محرمانه برای اشخاص شناسایی‌شده در طول چرخه حیات زنجیره تأمین ICT و حتی در مواقع مناسب پس از اتمام چرخه حیات سامانه است.

علاوه بر پیاده‌سازی فرایند مدیریت اطلاعات ISO/IEC 15288 تعدادی از کنترل‌های استاندارد ISO/IEC 27002 راهنمای تکمیلی در این زمینه فراهم می‌کنند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۳-۷ فرایند سنجش

هدف از فرایند سنجش، تحلیل و گزارش داده‌های مرتبط با محصولات توسعه‌یافته و فرایندهای پیاده‌سازی‌شده در سازمان به‌منظور پشتیبانی از مدیریت مؤثر فرایندها و نمایش هدف‌دار کیفیت محصولات است. هیچ‌یک از جنبه‌های مربوط به زنجیره تأمین ICT در این فرایند سنجش وجود ندارد. استاندارد ISO/IEC 27004 درباره رویکرد سنجش امنیت اطلاعاتی که می‌تواند در مورد توسعه و پیاده‌سازی سنجه‌های ویژه برای پوشش مخاطرات امنیت اطلاعات در زنجیره تأمین ICT به کار گرفته شود راهنمایی ارائه می‌کند.

۶-۴ فرایندهای فنی

فرایندهای فنی الزامات را تعریف کرده، الزامات را به محصولات و خدمات تبدیل کرده و حفظ استفاده از محصولات و خدمات تا امحای آن‌ها را پوشش می‌دهند. این فرایندها مگر درصورتی‌که صراحتاً بیان شده باشد، برای هر دو طرف کارفرما و تأمین‌کننده کاربردپذیر هستند.

۶-۴-۱ فرایند تعریف الزامات ذینفع[1]

هدف از فرایند تعریف الزامات ذینفع در زمینه زنجیره تأمین اطلاعات تعریف الزامات برای محصولات یا خدمات ICT است که می‌توانند همزمان با مدیریت مناسب مخاطرات امنیت اطلاعات مربوط به زنجیره تأمین ICT، خدمات لازم برای کاربران و دیگر ذینفعان را در یک محیط تعریف‌شده فراهم کنند[2]. توصیه می‌شود کارفرمایان و تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند تعریف الزامات ذینفع برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

الف) تعریف و مستندسازی الزامات حفاظت اطلاعات بر مبنای نیازهای کارفرما، الزامات توافق، و اطلاعات و مستندات ارزیابی و برطرف‌سازی مخاطره در دسترس.

ب) شفاف‌سازی مخاطرات و تهدیداتی که متوجه مأموریت شده و به‌کارگیری این دانش در تعریف الزامات مربوط به امنیت تأمین‌کننده.

پ) تعریف و مستندسازی الزامات یکپارچگی داده و اطلاعات برای تأمین‌کننده شامل یکپارچگی کد.

ت) تعریف و مستندسازی الزامات دسترس‌پذیری اطلاعات و سامانه برای تأمین‌کنندگان محصولات و خدمات ICT.

ث) تعریف و مستندسازی الزامات محرمانگی اطلاعات برای تأمین‌کنندگان محصولات و خدمات ICT.

ج) تعریف و مستندسازی جنبه‌های امنیت اطلاعات از الزامات تحویل محصولات و خدمات ICT.

چ) تعریف و مستندسازی عواقب تخطی از الزامات امنیت اطلاعات در تحویل محصولات و خدمات ICT.

استاندارد ISO/IEC 27002 راهنمای ویژه تکمیلی درباره تنظیم انتظارات در طی فرایند تعریف الزامات ذینفع فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۴-۲ فرایند تحلیل الزامات

هدف از فرایند تحلیل الزامات در زمینه زنجیره تأمین ICT انتقال دید مبتنی بر الزامات خدمات را که در نزد ذینفع است، به دید فنی محصول موردنیاز است. انتقال می‌تواند همزمان با مدیریت مناسب مخاطرات امنیت اطلاعات مرتبط با زنجیره تأمین ICT کارفرما، موجب تحویل خدمات موردنظر شود. توصیه می‌شود کارفرمایان و تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند تحلیل الزامات برای پوشش مخاطرات ویژه امنیت اطلاعات در زنجیره تأمین ICT به کار گیرند.

الف) اطمینان از انتساب درجات متغیر اهمیت به عناصر با توجه به اهمیت و استفاده از هر عنصر.

ب) به‌کارگیری ملاحظات و ارزیابی‌های مخاطرات زنجیره تأمین ICT در تمامی الزامات مدیریتی، عملیاتی و فنی و فرایندهای کسب‌وکار به‌منظور محافظت از فرایندها، الزامات، و روش‌های اجرایی کسب‌وکار در برابر به خطر افتادن محرمانگی، یکپارچگی و دسترس‌پذیری.

1- ISO/IEC 15288
2- ISO/IEC 15288

پ) به کارگیری معیارهای طراحی دفاعی در تمامی الزامات فنی که موجب گزینه های طراحی برای عناصر، سامانه‌ها و فرایندهایی که قابلیت‌های مأموریت، کارایی سامانه یا محرمانگی، یکپارچگی و دسترس‌پذیری عنصر را حفظ می‌کنند می‌شوند.
ت) محافظت از الزامات و مستندات مربوط به آن‌ها در برابر افشا یا دسترسی که می‌تواند موجب از دست رفتن محرمانگی، یکپارچگی یا دسترس‌پذیری عناصر و سامانه‌ها از طریق مخاطرات مربوط به زنجیره تأمین ICT شود.
ث) پایش و ارزیابی مجدد الزامات فنی در حال تکامل و تنظیم روش‌های اجرایی مدیریت تغییر تأییدشده و الزامات حفاظت از عناصر و فرایندهای حیاتی در سراسر چرخه حیات عنصر.
ج) شناسایی مفاهیم عملیاتی و فرانامه‌های مرتبط با آن‌ها در موارد استفاده نادرست و سوءاستفاده.
استاندارد ISO/IEC 27002 راهنمای ویژه تکمیلی برای استفاده در طی فرایند تحلیل الزامات فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۴-۳ فرایند طراحی معمارانه

هدف از فرایند طراحی معمارانه در زمینه زنجیره تأمین ICT هماهنگی[1] راه‌حلی است که همزمان با مدیریت مناسب مخاطرات امنیت اطلاعات مرتبط با زنجیره تأمین ICT کارفرما، الزامات سامانه را برآورده کند[2].
توصیه می‌شود کارفرمایان و تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند طراحی معمارانه برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

الف) استفاده از فنون طراحی دفاعی برای پیش‌بینی بیشینه راه‌های ممکنی که می‌توان از محصول یا خدمت استفاده نادرست یا سوءاستفاده نمود و محافظت از محصول یا سامانه در برابر این نوع استفاده‌ها. اطمینان حاصل شود که معماری و طراحی فرانامه‌های عمدی و غیرعمدی را پوشش می‌دهند. طراحی‌ها بر مبنای میزان تحمل خطای بیان‌شده توسط کارفرما انتخاب شود و پذیرش مخاطراتی که به‌صورت کامل کنترل نشده‌اند برای مدیریت به‌صورت چکیده مستند شود.

ب) تعداد، اندازه و اجازه دسترسی به مؤلفه‌های حیاتی محدود شود.

پ) پیچیدگی طراحی، فرایندهای تولید و پیاده‌سازی طراحی را کاهش دهید. پیچیدگی اثرات منفی زیادی شامل جذب نیروی کار یا احتمال جذب نیروی کار بوده و این خود می‌تواند موجب مسائل محرمانگی، یکپارچگی و دسترس‌پذیری شود. انتقال سریع شکست‌ها به دلیل اتصال بالای عناصر و همچنین ایجاد موانع در راستای تحلیل ریشه شکست‌ها و وقایع از مشکلات دیگری هستند که در اثر پیچیدگی ایجاد می‌شوند.

1- synthesize
2- ISO/IEC 15288

ت) استفاده از سازوکارها و کنترل‌های امنیتی برای کاهش فرصت‌های سوءاستفاده از آسیب‌پذیری‌های زنجیره تأمین ICT. مثال‌های این مورد شامل کدگذاری، کنترل دسترسی، مدیریت شناسه، کشف سنجه‌هایی مانند سنجه‌های مربوط به کشف بدافزار یا دست‌کاری.

ث) مجزا کردن عناصر(با استفاده از فنونی مانند ماشین‌های مجازی[1]، قرنطینه‌ها[2]، جیلز[3]، جعبه‌های شن[4] و دروازه‌های[5] یک‌طرفه) را به‌منظور کاهش خسارتی که یک عنصر می‌تواند به سایر عناصر وارد کند.

ج) طراحی اقدامات متقابل و کاهش‌هایی در مقابل سوءاستفاده‌های بالقوه از ضعف‌ها و آسیب‌پذیری‌ها در ICT. مؤلفه‌هایی برای در برگرفتن فنون برنامه‌نویسی و پیکربندی‌ها و غیره طراحی شود.

چ) گنجاندن توانایی پیکربندی انزوای افزایش‌یافته سامانه یا عناصر سامانه، حتی اگر این کار قابلیت‌های سامانه را کاهش دهد (مانند ضد حمله‌ها تا زمانی که یک وصله[6] در دسترس قرار گیرد)

ح) طراحی عناصری برای مقاومت در برابر ورودی‌های خارج از محدوده(مانند ولتاژ اضافی، اعداد خارج از محدوده و مواردی از این دست).

خ) طراحی عناصری که غیرفعال کردن آن‌ها مشکل باشد و در صورت غیرفعال شدن روش‌های اطلاع مانند سلسله‌های ممیزی، شواهد یا هشدار دست‌کاری و غیره را راه‌اندازی کنند.

د) طراحی سازوکارهای تحویل به منظور اجتناب از دسترسی یا افشای فرایندهای تحویل عنصر یا سامانه و استفاده از عنصر طی فرایند تحویل.

ذ) گنجاندن سامانه‌های زمان شکست[7]/ افزونه یا سامانه‌ها یا عناصر سامانه جایگزین در جای مناسب و تضمین این‌که سازوکارهای زمان شکست یا افزونه همزمان با سامانه یا عناصر اصلی از کار نمی‌افتند.

ر) تعریف و/یا استفاده از واسط‌های فنی مبتنی بر استاندارد و الزامات فرایند به‌منظور فراهم کردن گزینه‌هایی برای تغییر فرایندها یا تغییر/جایگزینی عناصری که تسخیرها در آن‌ها اتفاق می‌افتند.

ز) طراحی کنترل‌های اعتبارسنجی مرتبط به‌منظور استفاده در طی پیاده‌سازی و عملیات.

۶-۴-۴ فرایند پیاده‌سازی

هدف از فرایند پیاده‌سازی درک یک عنصر ویژه از سامانه است[8]. توصیه می‌شود تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند طراحی معمارانه برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

1- Virtual Machines
2- quarantines,
3- Jails
4- SandBoxes
5- Gateways
6- Patch
7- Fail-Over
8- ISO/IEC 15288

الف) پیاده‌سازی معماری و طراحی که الزامات مرتبط با زنجیره تأمین ICT برای محصولات و خدمات را در پوشش دهد.
ب) شناسایی انحرافات از الزامات مربوط به زنجیره تأمین اطلاعات و پیاده‌سازی کاهش مناسب و مستندسازی این اطلاعات.
پ) در جای ممکن و مناسب، با استفاده از زبان‌های برنامه‌نویسی طراحی سخت‌افزار و نرم‌افزار را به صورتی پیاده‌سازی نمایید که به‌منظور کاهش احتمال ضعف‌ها و خطرهای مربوط به زنجیره تأمین اطلاعات از ساختارهای کدگذاری که به‌صورت ذاتی غیر امن هستند اجتناب شود.
ت) شناسایی و پیاده‌سازی استانداردهای واسط در هر جا که عملی باشد به‌منظور ترویج مقاومت سامانه و عنصر و قابلیت استفاده مجدد عنصر.
ث) اعتبارسنجی پیاده‌سازی در مراحل مناسب و تعریف‌شده با استفاده از آزمون‌های اعتبارسنجی طراحی‌شده مانند:
ج) استفاده از فنون متنوع آزمون شامل آزمون فاز[1]، آزمون تحلیل ایستا[2]، و آزمون پویا به‌منظور شناسایی و رفع ضعف‌ها و آسیب‌پذیری‌ها.
چ) استفاده از آزمون‌های مثبت و منفی مناسب برای درستی‌سنجی این‌که سامانه یا مؤلفه منطبق با الزامات و بدون کارکرد اضافی عمل می‌کند.
ح) پایش رفتار غیرمنتظره یا نامطلوب در زمان آزمون، مانند رفتار شبکه (به‌عنوان‌مثال تماس غیرمنتظره با خانه، یا باز شدن درگاه شبکه)، رفتار سامانه پرونده (مانند خواندن یا نوشت اطلاعات در پرونده‌ها یا فهرست‌های راهنما[3])، شرایط رقابتی و بن‌بست‌ها[4].
خ) محافظت از دسترسی به موارد و نتایج آزمون. ذخیره موارد آزمون و نتایج در یک سامانه کنترل منبع و محافظت مشابه از نحوه محافظت از کد منبع و نبشته‌های ساخت[5].
د) تضمین دسترس‌پذیری عناصر لازم و تأمین مستمر آن‌ها در هنگام رویداد تسخیر سامانه/عنصر از طریق تنوع تأمین(به‌ویژه در مورد کارکردهای مربوط به کالا یا در رویدادهای تسخیر یا دست‌کاری سازوکارهای تحویل)
ذ) تضمین حذف یا غیرفعال کردن کارکردهای غیرضروری که در پیاده‌سازی‌های آماده تجاری که برای پوشش چندین کاربرد یا هدف طراحی می‌شوند شایع است. درصورتی‌که این کارکردها به‌صورت فعال رها شوند، می‌توانند امکان دسترسی غیرمجاز به سامانه یا انجام گزینه‌ای که دسترس‌پذیری دیگر گزینه‌ها را کاهش می‌دهد را فراهم کند.
ر) محصولات و/یا عناصر ویژه پیاده‌سازی را با توجه به توافقنامه مستندسازی نمایید.

1 - Fuzz testing
2 - Static analysis testing
3- Directory
4- Dead lock
5- Build script

استاندارد ISO/IEC 27002 راهنمای ویژه تکمیلی برای تنظیم انتظارات در طی فرایند پیاده‌سازی فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۴-۵ فرایند یکپارچه‌سازی

هدف از فرایند یکپارچه‌سازی، هم‌گذاری[1] محصول یا خدمت برای تحویل به صورتی است که منطبق با طراحی معمارانه باشد[2].

یادآوری - استاندارد ISO/IEC 15288 هدف از فرایند یکپارچه‌سازی را به شکل زیر بیان می‌کند.

هدف از فرایند یکپارچه‌سازی، سرهم‌بندی یک محصول یا خدمت به صورتی است که منطبق با طراحی معمارانه باشد.

توصیه می‌شود کارفرمایان و تأمین‌کنندگان جنبه‌های زیر از فرایند یکپارچه‌سازی برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

الف) یکپارچه‌سازی با سامانه‌های موجود باید شامل فعالیت‌های بند ۶-۴-۴ با توجه به ویژگی‌های یکپارچه‌سازی شوند؛

ب) توصیه می‌شود در مورد فعالیت‌های بند ۶-۴-۴ که طی یکپارچه‌سازی به کار گرفته شده و سامانه‌های موجودی که قبل از پیاده‌سازی استفاده می‌شده‌اند، مستندسازی صورت گیرد.

۶-۴-۶ فرایند درستی‌سنجی

هدف از فرایند درستی‌سنجی تأیید برآورده‌شدن الزامات طراحی مشخص‌شده به‌وسیله محصول یا خدمت موردنظر است[3].

یادآوری - استاندارد ISO/IEC 15288 هدف از فرایند درستی‌سنجی را به شکل زیر بیان می‌کند.

هدف از فرایند درستی‌سنجی تأیید برآورده‌شدن الزامات طراحی مشخص‌شده به‌وسیله سامانه موردنظر است.

توصیه می‌شود فرایند درستی‌سنجی شامل سنجش صحت اطلاعات قبل از اکتساب که میان کارفرما و تأمین‌کننده به اشتراک گذاشته شده است و توسعه الزامات درستی‌سنجی بر مبنای بندهای ۶-۲، ۶-۳ و ۶-۴ باشد.

توصیه می‌شود تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند درستی‌سنجی برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

الف) درستی‌سنجی و اعتبارسنجی این‌که الزامات امنیت زنجیره تأمین اطلاعات رعایت شده‌اند.

ب) درستی‌سنجی این‌که فعالیت‌های پشتیبانی تأمین‌کننده با اهداف امنیت اطلاعات و محصول کارفرما هم‌راستا هستند.

1- Assemble
2 - ISO/IEC 15288
3- ISO/IEC 15288

پ) درستی‌سنجی این‌که روش‌های اجرایی امنیتی الزام‌شده از سوی تأمین‌کننده، اجرا شده و کارکنان برای پیاده‌سازی آن‌ها آموزش دیده‌اند.
ت) درستی‌سنجی این‌که مستند کارکردها و ویژگی‌های امنیت تأمین‌کننده، پیوند میان ویژگی‌های محصول نتایج معماری، طراحی، الزامات، کد، آزمون‌ها و نتایج آزمون را برقرار می‌نمایند.
ث) درستی‌سنجی این‌که تأمین‌کننده فعالیت‌های درستی‌سنجی و اعتبارسنجی را به‌منظور تضمین اعمال کنترل‌ها اجرا کرده و این فعالیت‌ها به‌صورت مطلوب کار کرده و الزامات کارفرما را رعایت می‌کند.
ج) درستی‌سنجی این‌که زنجیره حفاظت میان سازمان‌ها نگهداری می‌شود.
چ) انجام ارزیابی و اعتبارسنجی کد با استفاده از ابزار و فنون مختلف مانند بازنگری‌های متناظر[1]، بازرسی دستی کد، تحلیل کد ایستا، تحلیل کد پویا، تحلیل کد دودویی، و ابزار پوشش.
ح) انجام پویش آسیب‌پذیری شبکه و برنامه کاربردی وب
خ) انجام پویش بدافزار
د) اجرای ابزارهای اعتبارسنجی انطباق
ذ) انجام آزمون فشار[2]
ر) امتحان گواهی‌ها یا مجوزهای فراهم‌شده توسط تأمین‌کنندگان:
۱) در مورد ادعاهای تأمین‌کننده درباره انطباق با روش‌های اجرایی امنیتی یا کسب‌وکار، یکپارچگی محصول یا زنجیره حفاظت؛
۲) اعطاشده به محصول برای ارزیابی تأثیر ادعاها در مورد مخاطرات کارفرما، یا تناسب محصول با هدف مشخص مرتبط با کاربرد موردنظر کارفرما.
استاندارد ISO/IEC 27002 راهنمای ویژه تکمیلی برای تنظیم انتظارات در طی فرایند درستی‌سنجی فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۴-۷ فرایند انتقال

هدف از فرایند انتقال ایجاد قابلیتی برای تأمین یا دریافت محصولات و خدمات مشخص‌شده توسط الزامات ذینفع در محیط عملیاتی است[3].

یادآوری – استاندارد ISO/IEC 15288 هدف از فرایند انتقال را به شکل زیر بیان می‌کند.

هدف از فرایند انتقال ایجاد قابلیتی برای تأمین خدمات مشخص‌شده توسط الزامات ذینفع در محیط عملیاتی است.

توصیه می‌شود کارفرمایان موارد زیر را به‌عنوان قسمتی از فرایند انتقال برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

1- Peer review
2- Stress testing
3 - ISO/IEC 15288

الف) گنجاندن نحوه درخواست جایگزینی، اضافه کردن به موجودی به شکل مناسب (شامل مکان‌های ذخیره و محافظت از ذخیره)، خط‌مشی‌های دریافت(دانستن این‌که موجودی به سمت چه کسی باید برود، چه زمانی می‌رسد، چه کسی آن را اداره می‌کند، مکان آن کجاست و این‌که آیا موجودی دریافت‌شده با آنچه سفارش داده شده است، مطابقت دارد یا خیر) و خط‌مشی‌های شمارش/حسابداری موجودی.

ب) ثبت کردن محصولات و عناصر در سامانه مدیریت موجودی سازمان.

پ) طراحی سازوکارهایی برای کاهش مخاطرات دسترسی غیرمجاز به سامانه محصولات و خدمات طی فرایند تحویل.

ت) پیاده‌سازی فرایندهای تحویل برای انتقال عمدی منطقی و فیزیکی و دریافت عناصر توسط افراد مجاز.

ث) ایجاد فنون غیر مخرب یا سازوکارهایی برای تعیین این‌که دسترسی غیرمجازی در سراسر فرایند تحویل وجود دارد یا خیر.

ج) تصریح سطح قابل‌قبول امنیت و کیفیت اطلاعات برای پایش تحویل منطقی محصولات و خدماتی که لازم است از پایگاه‌های تأییدشده و صحت‌سنجی‌شده بارگیری شوند. الزام کدگذاری عناصر(نرم‌افزار، وصله‌های نرم‌افزاری و غیره) در انتقال و سایر بخش‌های تحویل در نظر بگیرید.

چ) ایجاد فرایند و قابلیتی برای حفاظت از محصولات نرم‌افزاری از بدافزارها.

ح) ایجاد یک فرایند و قابلیت برای درستی‌سنجی نشانه‌هایی مانند امضای دیجیتال و برچسب‌های هولوگرام برای عناصر حیاتی.

توصیه می‌شود تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند انتقال برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

الف) ایجاد فرایند و قابلیتی برای حفاظت از محصولات نرم‌افزاری از بدافزارها.

ب) در نظر گرفتن الزام کدگذاری عناصر(نرم‌افزار، وصله‌های نرم‌افزاری و غیره) در انتقال و سایر بخش‌های تحویل.

پ) کاهش مخاطرات جعل و فراهم کردن اجازه صحت‌سنج توسط کارفرما، استفاده از فنونی مانند نشانه‌هایی که به‌سختی فراموش می‌شوند[1](امضای دیجیتال و برچسب‌های هولوگرام) برای عناصر حیاتی، نشانه‌گذاری رقمی شامل شناسه عرضه‌کننده، مؤلفه‌های نرم‌افزاری با قابلیت امضای محرمانه و استفاده از چکیده‌سازهای رقمی.

ت) استقرار فرایندهای تحویل ویژه به شکلی که کارفرما قابلیت تأیید این‌که محصول از تأمین‌کننده خاصی می‌آید را داشته باشد.

ث) ایجاد سازوکارهای ضد دست‌کاری برای جلوگیری و کشف شامل بسته‌بندی مقاوم در برابر دست‌کاری و مشهودکننده دست‌کاری (مانند نوار یا مهر دست‌کاری). حذف یا جایگزینی این موارد نباید بدون برجا گذاشتن شواهد ساده باشد.

1- difficult-to-forge marks

استاندارد ISO/IEC 27002 راهنمای ویژه تکمیلی برای تنظیم انتظارات در طی فرایند انتقال فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۴-۸ فرایند اعتبارسنجی

هدف از فرایند اعتبارسنجی در زمینه زنجیره تأمین ICT فراهم کردن مدارکی هدف‌دار مبنی بر آن است که محصولات و خدمات با الزامات ذینفع مطابقت داشته و به استفاده موردنظر خود در محیط عملیاتی موردنظر دست می‌یابند.[1]

یادآوری – استاندارد ISO/IEC 15288 هدف از فرایند انتقال را به شکل زیر بیان می‌کند.

هدف از فرایند انتقال ایجاد قابلیتی برای تأمین خدمات مشخص‌شده توسط الزامات ذینفع در محیط عملیاتی است.

هدف از فرایند اعتبارسنجی در زمینه زنجیره تأمین ICT فراهم کردن مدارکی هدف‌دار مبنی بر آن است که خدمات تأمین‌شده توسط یک سامانه در زمان استفاده با الزامات ذینفع مطابقت داشته و به استفاده موردنظر خود در محیط عملیاتی موردنظر دست می‌یابند.

توصیه می‌شود این فرایند بر مبنای شرح یا الزامات محصول تأمین‌کننده و قرارداد میان کارفرما و تأمین‌کننده تعیین کند که محصول دریافتی اصل و بدن تغییر است تا اطمینانی از عدم تغییر محصول در نزد کارفرما ایجاد شود. همچنین، فرایند بیان‌شده بهتر است شامل توسعه آزمون‌هایی که از طریق استفاده محصول توسط کارفرما اعتبارسنجی می‌کنند باشد. به ویژه، توصیه می‌شود کارفرمایان موارد زیر را به‌عنوان قسمتی از فرایند اعتبارسنجی برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

الف) درستی‌سنجی و اعتبارسنجی این‌که الزامات امنیتی اطلاعات زنجیره تأمین ICT رعایت شده‌اند؛

ب) توسعه فرایندهایی برای استفاده رویه‌هایی برای به‌کارگیری ابزارهای اعتبارسنجی محصولات و نرم‌افزارهای غیرتهاجمی از یک مؤسسه تولیدکننده تجهیزات اصل(OEM)[2] در جای مناسب که قابلیت کشف جعل یا نفوذ در محصولات را داشته باشد.

پ) انجام آزمون در زمان مرحله‌های دریافت، توسعه و عملیات سامانه کارفرما. سعی در کشف جعل یا نفوذ در محصول شامل موارد زیر:

۱) انجام بازرسی‌های سخت‌افزاری و نرم‌افزاری برای مؤلفه‌های اصل با استفاده از راهنما و ابزارهای فراهم‌شده توسط تأمین‌کننده، شخص سوم، یا کارفرما (مانند بازرسی‌های دستی کد)

۲) انجام بازرسی‌های ضد بدافزار.

۳) انجام پویش‌های آسیب‌پذیری.

ت) استفاده از مستندسازی محصول و برنامه‌های کارفرما برای شناسایی و آزمون مؤلفه‌های حیاتی.

1- ISO/IEC15288

2 - Original Equipment Manufacturer

ث) انجام ارزیابی و درستی‌سنجی کد با استفاده از ابزارهای و فنون مختلف مانند تحلیل کد ایستا، تحلیل کد پویا، تحلیل کد دودویی و ابزارهای پوشش کد.
ج) انجام آزمون فشار.
چ) اجرای ابزارهایی برای جمع‌آوری مدارک تغییرات ناشی از فعالیت‌های نگهداری از راه دور.

۶-۴-۹ فرایند عملیات

هدف از فرایند عملیات، تحویل محصولات و خدمات در انطباق با الزامات توافق شده است.
یادآوری - استاندارد ISO/IEC 15288 هدف از فرایند عملیات را به شکل زیر بیان می‌کند.

هدف از فرایند عملیات، استفاده از سامانه در جهت تحویل خدمات آن است.
توصیه می‌شود کارفرمایان و تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند عملیات برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:
الف) تأمین‌کنندگان باید عناصر را به‌صورت امن در حالت پیش‌فرض در سطحی از امنیت که برای الزامات کارفرما مناسب باشد ارائه دهند.
ب) گنجاندن فعالیت‌های قابل‌کاربرد یکپارچه‌سازی سامانه و گسترش کد به صورت سفارشی به‌عنوان کارهای به‌روزرسانی و نگهداری در الزامات عملیاتی سامانه.
پ) انجام تمام فعالیت‌های امنیت اطلاعات قابل‌کاربرد و پیاده‌سازی الزامات امنیت اطلاعات کاربردپذیر در عملیات.
استاندارد ISO/IEC 27002 راهنمای ویژه تکمیلی برای تنظیم انتظارات در طی فرایند عملیات فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۴-۱۰ فرایند نگهداشت

هدف از فرایند نگهداشت در زمینه زنجیره تأمین ICT حفظ قابلیت سامانه و مؤلفه‌های آن برای فراهم کردن خدمتی همزمان با مدیریت مناسب مخاطرات امنیت اطلاعات زنجیره تأمین ICT کارفرما است.
توصیه می‌شود کارفرمایان و تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند نگهداشت برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:
الف) استفاده از بندهای تهیه به برای کاهش مخاطرات زنجیره تأمین ICT در توافق رسمی خدمت و نگهداشت با تأمین‌کننده.
ب) در زمان اکتساب عناصر تولیدکنندگان تجهیزات اصل (OEM) شامل عناصر تجدید شده، در صورت امکان یک رابطه قراردادی با تولیدکننده اصلی یا مبتکری که پشتیبانی امتحان‌شده و شایسته‌ای فراهم می‌کند ایجاد شود.
پ) در نظر گرفتن خریداری و ذخیره قطعات یدکی هنگامی‌که به‌صورت گسترده در دسترس و قابل درستی‌سنجی بوده و می‌توانند توسط کارکنان آموزش‌دیده و صاحب دانش مجاز خدمات نصب شوند.

ت) در نظر گرفتن این مخاطرات که ممکن است کارکنان آموزش دیده و صاحب دانش مجاز خدمات به ویژه در پایان طول عمر عنصر در دسترس نباشند.
ث) در نظر گرفتن مخاطرات زنجیره تأمین ICT در هنگام اکتساب مؤلفه‌های جایگزین با اضافه‌کردن/ تغییر/به‌روزرسانی فیلد، به‌ویژه اگر این مؤلفه‌ها فرایندهای سنتی اکتساب که مخاطرات زنجیره تأمین را بررسی می‌کنند طی نکرده باشند.
ج) ترجیح موافقت‌نامه‌های خدمت/نگهداشت رسمی در صورت امکان. به‌عنوان‌مثال، استفاده از تأمین‌کنندگان قطعات یدکی ویژه یا کیفیت‌سنجی شده، ارائه سوابق کامل تغییرات انجام‌شده در طی نگهداشت (مانند سلسله‌های ممیزی یا رخداد نگار تغییر) و بازنگری تغییرات انجام‌شده طی نگهداشت.
چ) ایجاد و پیاده‌سازی توافق برای پشتیبانی خوب و مناسب شامل عناصر تجدیدشده و/یا بازیابی‌شده. الزام کردن تولیدکننده اصلی به شفاف‌سازی را در مواقع مناسب در نظر گرفته شود.
ح) شناسایی روش‌هایی برای بررسی این‌که کارکنان خدمات اصالت‌سنجی‌شده و مجاز به انجام کارهای خدمات در حال حاضر هستند.
خ) توسعه و پیاده‌سازی رویکردی برای اداره و پردازش ناهنجاری‌های زنجیره تأمین ICT پس از عملیاتی شدن آن.
د) پایش سلامت کسب‌وکار تأمین‌کننده ـ شامل این‌که آیا آن‌ها نامزدی برای ادغام یا اکتساب از سوی سازمان‌های دیگر هستند یا خیر و این‌که آیا با مشکلات مالی مواجه هستند.
ذ) ایجاد مستندات برای هر عنصر در حال خدمت‌رسانی که دیگر از سوی تأمین‌کننده پشتیبانی نمی‌شود.
ر) پیاده‌سازی و اجرای خط‌مشی‌هایی درباره مدیریت به‌روزرسانی‌ها و وصله‌های نرم‌افزار.
ز)ایجاد ذخیره کافی از قطعات یدکی مورد اطمینان و نگهداشت قطعات برای مدت‌ها بعد از دوره حیات عنصر.
ژ) ایجاد مستندات برای هر عنصر در حال خدمت‌رسانی که دیگر از سوی تأمین‌کننده پشتیبانی نمی‌شود.
استاندارد ISO/IEC 27002 راهنمای ویژه تکمیلی برای تنظیم انتظارات در طی فرایند نگهداشت فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

۶-۴-۱۱ فرایند امحا[1]

هدف از فرایند امحا در زنجیره تأمین ICT خاتمه دادن به وجود عناصر زنجیره تأمین ICT است.[2]
یادآوری – استاندارد ISO/IEC 15288 هدف از فرایند را به شکل زیر بیان می‌کند.

هدف از فرایند امحا پایان دادن به وجود یک هستار سامانه است.

1- Disposal
2- ISO/IEC 15288

امحا می‌تواند در هر نقطه‌ای از چرخه حیات سامانه یا عنصر رخ داده و شامل رسانه‌های الکترونیکی و غیرالکترونیکی شود. توصیه می‌شود کارفرمایان و تأمین‌کنندگان موارد زیر را به‌عنوان قسمتی از فرایند امحا برای پوشش مخاطرات خاص مربوط به زنجیره تأمین ICT در نظر بگیرند:

الف) نگهداری زنجیره حفاظت برای عناصری که قرار است امحا شوند، به‌منظور کاهش مخاطرات تسخیر مانند داده‌های قابل‌شناسایی شخصی[1] یا مالکیت معنوی.

ب) تشویق به انتخاب عناصری که می‌توانند به صورتی امحا شوند که اطلاعات حفاظت‌شده افشا نشوند. مانند عناصری که امکان خارج کردن داده‌ها از حالت بارگذاری را پیش از امحا فراهم می‌کنند یا عناصری که پاکسازی آن‌ها پیش از امحا ساده است.

پ) منع کردن انتقال یا توزیع داده‌ها یا عناصر حساس کارفرما یه اشخاص غیرمجاز یا نامشخص در طی فعالیت‌های امحا.

ت) در صورت لزوم برای بازرسی قانونی[2] یا برای کشف جعل، عناصر برای امحا به یک مخزن اختصاصی انتقال داده شوند و زنجیره حفاظت نگهداری شود.

ث) رویه‌هایی برای امحای دائمی عناصر پیاده‌سازی شود.

ج) متعهدکردن کارکنان خدمت مورداعتماد و آموزش‌دیده و تنظیم انتظارات برای روش‌های اجرایی به صورتی‌که با سیاست امحا منطبق باشد. از طریق ارزیابی‌ها بررسی شود که روش‌های اجرایی رعایت شده‌اند.

استاندارد ISO/IEC 27002 راهنمای ویژه تکمیلی برای تنظیم انتظارات در طی فرایند امحا فراهم می‌کند. نگاشت بند ۶ استاندارد ISO/IEC 27036-3 به کنترل‌های استاندارد ISO/IEC 27002 در پیوست ب آمده است.

1- personally identifiable data
2- Forensic investigation

پیوست الف

(اطلاعاتی)

خلاصه فرایندهای تأمین و اکتساب از ISO/IEC 15288 و ISO/IEC 12207

فرایندهای اکتساب و تأمین استانداردهای ISO/IEC 15288 و ISO/IEC 12207 مکمل یکدیگر هستند. به‌عبارت‌دیگر، هر یک از فعالیت‌های اکتساب، دارای فعالیت تأمین معادل خود است.

توجه شود که ISO/IEC15288 و ISO/IEC 12207 در قالب‌هایی که دارای اندکی تفاوت هستند نوشته شده‌اند. ISO/IEC15288 از فهرست‌های تودرتو استفاده می‌کند، در حالی که ISO/IEC121207 از شماره‌گذاری زیاد زیربندها استفاده می‌کند.

جدول زیر فرایندها را به‌منظور نمایش روابط مکمل میان کارفرما و تأمین‌کننده در قالب کنار هم ارائه می‌دهد. علاوه بر آن، ISO/IEC 12207 نسخه ویژه‌ای از ISO/IEC 15288 را ارائه می‌کند.

جدول الف ـ۱ـ مخاطرات نمونه امنیت اطلاعات برای اکتساب خدمات

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
۶ـ۱ـ۱ فرایند اکتساب ۶-۱-۱-۱ قصد قصد از فرآیند اکتساب، کسب محصول یا خدمتی بر اساس نیازمندی‌های کارفرما است.	۶ـ۱ـ۲ فرایند تأمین ۶-۱-۲-۱ قصد قصد از فرآیند تأمین، تأمین یک محصول یا خدمت برای کارفرما بر اساس نیازمندی‌های توافق شده است.	۶ـ۱ـ۱ فرایند اکتساب ۶-۱-۱-۱ قصد قصد از فرایند اکتساب تهیه محصول و/یا خدمت مطابق به نحوی است که نیازهای بیان‌شده توسط کارفرما را برآورده کند. این فرایند با شناسایی نیازهای مشتری آغاز شده و با پذیرش محصول و/یا خدمت موردنیاز کارفرما پایان می‌یابد.	۶ـ۱ـ۱ فرایند تأمین ۶-۱-۲-۱ قصد قصد از فرایند تأمین، فراهم کردن محصول یا خدمت مطابق با الزامات توافق‌شده برای کارفرماست.
۶ـ۱ـ۱ـ۲ دستاوردها در نتیجه‌ی اجرای موفق فرآیند اکتساب: الف) راهبردی برای اکتساب تدوین می‌شود. ب) یک یا چند تأمین‌کننده انتخاب می‌شوند. پ) ارتباط با تأمین‌کننده برقرار و حفظ می‌شود.	۶ـ۱ـ۲ـ۲ دستاوردها در نتیجه‌ی اجرای موفق فرآیند تأمین: الف) کارفرمای محصول یا خدمت شناسایی می‌شود. ب) به تقاضای کارفرما پاسخ داده می‌شود. پ) توافق‌نامه‌ای برای تأمین محصول یا خدمت بر	۶ـ۱ـ۱ـ۲ دستاوردها به‌عنوان نتیجه پیاده‌سازی موفق فرایند اکتساب: الف) نیازها، اهداف، معیارهای پذیرش محصول و/یا خدمت و راهبردهای اکتساب تعریف می‌شود. ب) توافقی توسعه می‌شود که به‌صورت شفاف انتظارات،	۶ـ۱ـ۲ـ۲ دستاوردها به‌عنوان نتیجه پیاده‌سازی موفق فرایند تأمین: الف) کارفرمایی برای محصول یا خدمت شناسایی شده است. ب) پاسخی به درخواست کارفرما داده می‌شود. پ) توافقی میان کارفرما و تأمین‌کننده برای توسعه،

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
ت) توافق‌نامه‌ای به‌منظور اکتساب محصول یا خدمتی مطابق با معیارهای پذیرش تعریف‌شده ، منعقد می‌شود. ث) محصول یا خدمتِ منطبق با توافق‌نامه پذیرفته می‌شود. ج) پرداخت یا سایر ملاحظات انجام می‌گیرد.	اساس معیارهای پذیرش تعریف‌شده منعقد می‌شود. ت) ارتباط با کارفرما برقرار و حفظ می‌شود. ث) محصول یا خدمت منطبق با توافق‌نامه بر اساس رویه‌ها و شرایط تحویلِ توافق شده، تأمین می‌شود. ج) مسؤولیت محصول یا خدمت کسب‌شده، همان‌گونه که در توافق‌نامه تصریح شده است، به کارفرما انتقال می‌یابد. چ) پرداخت‌ها یا سایر ملاحظات توافق شده دریافت می‌شود.	مسئولیت‌ها و تعهدات کارفرما و تأمین‌کننده را به‌صورت شفاف بیان می‌کند. پ) یک یا چند تأمین‌کننده انتخاب می‌شوند. ت) محصول و/یا خدمتی که نیازهای بیان‌شده از سوی کارفرما را برآورده کند، تهیه می‌شود. ث) اکتساب به نوعی پایش می‌شود که محدودیت‌های مشخص‌شده مانند هزینه، برنامه زمانی و کیفیت رعایت می‌شود. ج) اقلام تحویلی توسط تأمین‌کننده موردپذیرش قرار می‌گیرد؛ و چ) تمامی آیتم‌های باز نتیجه رضایت‌بخشی مطابق توافق منعقدشده میان کارفرما و تأمین‌کننده دارند.	نگهداشت، عملیاتی کردن، بسته‌بندی، تحویل و نصب محصول و/یا خدمت منعقد می‌شود. ت) محصول یا خدمتی که الزامات توافق‌شده را برآورده کند توسط تأمین‌کننده توسعه داده می‌شود. ث) محصول و/یا خدمت منطبق با الزامات توافق‌شده به کارفرما تحویل می‌شود. و ج) محصول مطابق با الزامات توافق‌شده نصب می‌شود.
۶ـ۱ـ۱ـ۳ فعالیت‌ها و کارها کارفرما باید فعالیت‌ها و کارهای زیر را در انطباق با خط‌مشی‌ها و رویه‌های کاربست پذیر سازمانی، بر اساس فرآیند اکتساب انجام دهد. یادآوری فعالیت‌ها و کارها در این فرآیند می‌توانند برای یک یا چند تأمین‌کننده به کار روند. الف) آمادگی برای اکتساب. این فعالیت شامل کارهای زیر می‌شود: ۱) تدوین راهبردی برای	۶ـ۱ـ۲ـ۳ فعالیت‌ها و کارها تأمین‌کننده باید فعالیت‌ها و کارهای زیر را در انطباق با خط‌مشی‌ها و رویه‌های کاربست پذیر سازمانی و بر اساس فرآیند تأمین انجام دهد. الف) شناسایی فرصت‌ها .این فعالیت شامل کارهای زیر می‌شود: ۱) شناسایی موجود بودن و هویت کارفرمایی که یا خود نیازی به یک محصول یا خدمت دارد و یا نماینده‌ی سازمان یا سازمان‌هایی است	۶ـ۱ـ۱ـ۳ فعالیت‌ها و وظایف کارفرما باید فعالیت‌های زیر را مطابق با خط‌مشی‌ها و روش‌های اجرایی قابل‌کاربرد سازمانی با توجه به فرایند اکتساب پیاده‌سازی کند. یادآوری: فعالیت‌ها و وظایف این فرایند می‌توانند در مورد یک یا چند تأمین‌کننده اجرا شوند. ۶ـ۱ـ۱ـ۳ـ۱ آماده شدن برای اکتساب. این فعالیت شامل وظایف زیر است: ۶ـ۱ـ۱ـ۳ـ۱ـ۱ کارفرما فرایند اکتساب با شرح یک مفهوم	۶ـ۱ـ۲ـ۳ فعالیت‌ها و وظایف تأمین‌کننده باید فعالیت‌ها و وظایف زیر را مطابق با خط‌مشی‌ها و روش‌های اجرایی قابل‌کاربرد سازمانی با توجه به فرایند اکتساب پیاده‌سازی کند. ۶ـ۱ـ۲ـ۳ـ۱ شناسایی فرصت. این فعالیت، شامل وظیفه زیر است. ۶ـ۱ـ۲ـ۳ـ۱ـ۱ توصیه می‌شود تأمین‌کننده وجود یک کارفرما را به نمایندگی از یک یا چند سازمان که نیاز به یک محصول یا خدمت دارد تعیین کرده و کارفرمای بیان‌شده را شناسایی

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
چگونگی اجرای اکتساب. یادآوری این استراتژی دربردارنده‌ی ارجاع به مدل چرخه حیات، زمان‌بندی نقاط عطف و معیارهای انتخاب، در صورتی که تأمین‌کننده، بیرون از سازمان کارفرما باشد، است. ۲) آماده‌سازی درخواست برای تأمین محصول یا خدمت که دربردارنده‌ی تعریف نیازمندی‌ها است. یادآوری تعریف نیازمندی‌ها برای یک یا چند تأمین‌کننده فراهم شود .اگر تأمین‌کننده عاملی بیرونی باشد، درخواست می‌تواند شیوه‌های کسب‌وکار که انتظار می‌رود تأمین‌کننده با آن‌ها منطبق باشد و نیز معیارهای انتخاب تأمین‌کننده را دربرداشته باشد.	که آن‌ها به یک محصول یا خدمت نیاز دارند. یادآوری در مورد محصول یا خدمتی که برای مصرف‌کننده ایجاد می‌شود، عاملی[1] مانند بخش بازاریابی در سازمان تأمین‌کننده، می‌تواند در نقش کارفرما ظاهر شود.	یا نیاز برای اکتساب، توسعه یا ارتقاء یک سامانه، محصول نرم‌افزاری یا خدمت نرم‌افزاری آغاز می‌کند. ۶ـ۱ـ۱ـ۳ـ۱ـ۲ کارفرما باید الزامات سامانه را تعریف و تحلیل کند. توصیه می‌شود الزامات سامانه شامل الزامات مربوط به کسب‌وکار، سازمان و کاربر و مواردی مانند امنیت و دیگر الزامات حیاتی به همراه استانداردها و روش‌های اجرایی مربوط به طراحی، آزمون و انطباق باشند. ۶ـ۱ـ۱ـ۳ـ۱ـ۳ ممکن است کارفرما تعریف و تحلیل الزامات نرم‌افزاری را خود انجام داده و یا به یک تأمین‌کننده بسپارد. ۶ـ۱ـ۱ـ۳ـ۱ـ۴ درصورتی‌که کارفرما تحلیل الزامات سامانه یا نرم‌افزار را به تأمین‌کننده‌ای بسپارد باید اختیار تأیید الزامات تحلیل‌شده با کارفرما باشد. ۶ـ۱ـ۱ـ۳ـ۱ـ۵ فرایند فنی (زیربند ۶ـ۴) باید برای انجام وظایف زیربندهای ۶ـ۱ـ۱ـ۳ـ۱ـ۲ و ۶ـ۱ـ۱ـ۳ـ۱ـ۴ استفاده شود. ممکن است کارفرما از فرایند تعریف الزامات ذینفعان برای ایجاد الزامات مشتری استفاده	کند. یادآوری ـ برای محصول یا خدمتی که برای مصرف‌کنندگان توسعه داده شده است، ممکن است عاملی مانند واحد بازاریابی در داخل سازمان تأمین‌کننده نماینده کارفرما باشد.

1- Agent

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
		کند. ۶ـ۱ـ۱ـ۳ـ۱ـ۶ کارفرما باید گزینه‌هایی را با توجه به معیارهایی شامل مخاطرات، هزینه و فایده برای اکتساب در نظر گیرد. این گزینه‌ها عبارت‌اند از: الف) خرید یک محصول نرم‌افزاری آماده که الزامات را برآورده می‌کند. ب) توسعه محصول نرم‌افزاری یا تهیه خدمت نرم‌افزاری به‌صورت داخلی. پ) توسعه محصول نرم‌افزاری یا تهیه خدمت نرم‌افزاری از طریق قرارداد. ت) ترکیبی از بندهای الف، ب، پ بالا. ث) ارتقاء یک محصول یا خدمت نرم‌افزاری موجود. ۶ـ۱ـ۱ـ۳ـ۱ـ۷ هنگامی‌که قصد اکتساب یک نرم‌افزار آماده وجود داشته باشد، کارفرما باید از ارضای شرایط زیر اطمینان حاصل کند: الف) الزامات محصول نرم‌افزاری برآورده شده‌اند. ب) مستندات موردنیاز در دسترس هستند. پ) حقوق استفاده، مالکیت، ضمانت و گواهی اختصاصی رعایت شده است. ت) برای پشتیبانی آینده محصول نرم‌افزاری برنامه‌ریزی شده است. ۶ـ۱ـ۱ـ۳ـ۱ـ۸ توصیه می‌شود	

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
		کارفرما یک برنامه اکتساب را آماده‌سازی، مستند و اجرا کند. برنامه بیان‌شده باید شامل موارد زیر باشد: الف) الزاماتی برای سامانه. ب)به‌کارگیری طرح‌ریزی‌شده سامانه. پ) نوع قراردادی که قرار است به کار بسته شود. ت)مسئولیت‌های سازمان‌های درگیر. ث) مفهوم پشتیبانی برای استفاده در آینده. ج)مخاطرات درنظرگرفته‌شده علاوه بر روش‌هایی برای مدیریت مخاطرات. ۶ـ۱ـ۱ـ۳ـ۱ـ۹ کارفرما باید راهبردها و شرایط پذیرش (معیارها) را تعریف و مستندسازی کند. ۶ـ۱ـ۱ـ۳ـ۱ـ۱۰ توصیه می‌شود کارفرما الزامات اکتساب را مستندسازی کند (مانند درخواست برای پیشنهاد (RFP)[1]). محتوای این مستندات به گزینه‌های انتخاب‌شده در زیر بند ۶ـ۱ـ۱ـ۳ـ۱ـ۶ بستگی دارد. مستندات اکتساب در مواقع مناسب بهتر است شامل موارد زیر باشند: الف) الزامات سامانه. ب) بیانیه محدوده. پ)دستورالعمل‌های	

1- Request For Proposal

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
		شرکت‌کنندگان مناقصه. ت) فهرست محصولات نرم‌افزاری. ث) قواعد و شرایط. ج) کنترل زیرقراردادها. چ) قیود فنی (مانند محیط مقصد) ۶ـ۱ـ۱ـ۳ـ۱ـ۱۱ توصیه می‌شود کارفرما تعیین کند که کدام‌یک از فرایندهای این استاندارد ملی برای اکتساب مناسب هستند و الزامات کارفرما برای متناسب‌سازی فرایندهای بیان‌شده را مشخص کند. توصیه می‌شود کارفرما مشخص کند که آیا هیچ‌یک از این فرایندها قرار است توسط شخصی غیر از تأمین‌کننده انجام شوند یا خیر. در این صورت ممکن است تأمین‌کنندگان در پیشنهادهای خود رویکرد خود در رابطه با پشتیبانی از کار اشخاص دیگر را ارائه کنند. کارفرما باید محدوده این وظایف را با ارجاع به قرارداد مشخص کند. ۶ـ۱ـ۱ـ۳ـ۱ـ۱۲ مستند اکتساب باید نقاط عطف قرارداد که باید در آن‌ها میزان پیشرفت تأمین‌کننده بازنگری و ممیزی شود را به‌عنوان قسمتی از پایش اکتساب تعریف کند (زیربندهای ۷ـ۲ـ۶ و ۷ـ۲ـ۷ را مشاهده نمایید)	

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
		۶ـ۱ـ۱ـ۳ـ۱ـ۱۳ توصیه می‌شود الزامات اکتساب برای انجام فعالیت‌های اکتساب به سازمان انتخاب‌شده داده شود.	
ب) آگهی کردن اکتساب و انتخاب تأمین‌کننده. این فعالیت شامل کارهای زیر می‌شود: ۱) اطلاع‌رسانی برای درخواست تأمین محصول یا خدمت به تأمین‌کنندگان شناسایی‌شده. یادآوری- این اقدام می‌تواند شرکای مدیریت زنجیره‌ی تأمین را که برای رسیدن به رویکردی جمعی یا هماهنگ در زمینه‌ی موضوعات مشترک فنی و بازرگانی با کارفرمایان و تأمین‌کنندگان وابسته به تبادل اطلاعات می‌پردازند را نیز در بر بگیرد.	ب) پاسخ به یک مناقصه . این فعالیت شامل کارهای زیر می‌شود: ۱) ارزیابی درخواست جهت تأمین یک محصول یا خدمت به‌منظور امکان سنجی و تعیین چگونگی پاسخ دهی به آن. ۲) آماده سازی پاسخی متناسب با درخواست.	۶ـ۱ـ۱ـ۳ـ۲ تبلیغ برای اکتساب. این فعالیت شامل وظایف زیر است: ۶ـ۱ـ۱ـ۳ـ۲ـ۱ کارفرما باید درخواست را به‌منظور تأمین محصول یا خدمت موردنظر به تأمین‌کنندگان شناسایی‌شده ارسال کند. یادآوری ـ این کار ممکن است شامل شراکت در مدیریت زنجیره تأمین باشد که با تأمین‌کنندگان و کارفرمایان مرتبط برای دستیابی به رویکرد هماهنگ یا جمعی در مورد مسایل فنی یا تجاری مشترک تبادل اطلاعات کند.	۶ـ۱ـ۲ـ۳ـ۲ مناقصه تأمین‌کننده. این فعالیت شامل وظایف زیر است: ۶ـ۱ـ۲ـ۳ـ۲ـ۱ توصیه می‌شود تأمین‌کننده بازنگری الزامات موجود در درخواست برای پیشنهاد را انجام داده و درآن خط‌مشی‌های سازمانی و دیگر مقررات را مدنظر قرار دهد. ۶ـ۱ـ۲ـ۳ـ۲ـ۲ تأمین‌کننده باید در مورد اعلام قیمت یا پذیرش قرارداد تصمیم‌گیری کند. ۶ـ۱ـ۲ـ۳ـ۲ـ۳ تأمین‌کننده باید پیشنهادی در پاسخ به درخواست برای پیشنهاد آماده کند.
۲) انتخاب یک یا چند تأمین‌کننده. یادآوری به‌منظور رسیدن به ارجاع کار رقابتی، پیشنهادهایی که از سوی تأمین‌کنندگان ارسال می‌شود، مورد ارزیابی قرار گرفته و با معیارهای انتخاب مقایسه می‌شود .هرگاه پیشنهادها، دربردارنده‌ی مواردی باشند که در معیارهای انتخاب دیده نشده است، آنگاه پیشنهادها با		۶ـ۱ـ۱ـ۳ـ۳ انتخاب تأمین‌کننده. این فعالیت شامل وظایف زیر است: ۶ـ۱ـ۱ـ۳ـ۱ توصیه می‌شود کارفرما رویه‌ای برای انتخاب تأمین‌کننده شامل معیارهای ارزیابی پیشنهاد و وزن‌دهی به میزان انطباق با الزامات ایجاد کند. ۶ـ۱ـ۱ـ۳ـ۲ کارفرما باید تأمین‌کننده‌ای را بر مبنای ارزیابی پیشنهادها و قابلیت‌ها و در انطباق با راهبردها و	

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
یکدیگر مورد مقایسه قرار می‌گیرند تا درجه مناسب بودن آن‌ها تعیین و به‌تبع آن تأمین‌کننده ترجیحی تعیین شود. توجیه رده‌بندی پیشنهادها اعلام می‌شود و تأمین‌کنندگان می‌توانند از این‌که چرا انتخاب شده‌اند یا نشده‌اند مطلع شوند.		شرایط پذیرش کارفرما انتخاب کند.	
پ) انعقاد توافق‌نامه .این فعالیت شامل کارهای زیر می‌شود: ۱) مذاکره با تأمین‌کننده برای (انعقاد) توافق‌نامه. یادآوری این توافق‌نامه از نظر رسمیت ممکن است از یک قرارداد مکتوب تا یک تفاهم شفاهی متغیر باشد . متناسب با سطح رسمیت، توافق‌نامه نیازمندی‌ها، نقاط عطف توسعه و تحویل، شرایط تصدیق، صحه‌گذاری و پذیرش، رویه‌های اداره موارد استثنایی، رویه‌های کنترل تغییر و زمان‌بندی پرداخت‌ها را تعیین می‌کند، به‌گونه‌ای که هر دو طرف توافق‌نامه مبنای اجرای توافق‌نامه را درک کنند .حقوق و محدودیت‌های مرتبط با	پ) انعقاد توافق‌نامه .این فعالیت شامل کارهای زیر می‌شود: ۱) مذاکره با کارفرما برای (انعقاد) توافق‌نامه. یادآوری این توافق‌نامه از نظر رسمیت ممکن است از یک قرارداد مکتوب تا یک تفاهم شفاهی متغیر باشد . تفاوت‌های میان درخواست اکتساب یا بیانیه‌ی سازمان‌دهی کار و قابلیت‌های بیان شده در پاسخ، هرکجا که لازم است، مورد مذاکره قرار می‌گیرد . تأمین‌کننده تأیید می‌کند که نیازمندی‌ها، نقاط عطف تحویل و شرایط پذیرش دست‌یافتنی هستند ، همچنین تأیید می‌کند که رویه‌های کنترل تغییر، رویه‌های اداره موارد استثنایی و همچنین	۶ـ۱ـ۱ـ۳ـ۴ قرارداد توافق. این فعالیت شامل وظایف زیر است: ۶ـ۱ـ۱ـ۳ـ۴_۱ ممکن است کارفرما اشخاص دیگر شامل تأمین‌کنندگان بالقوه یا هر شخص سوم لازم دیگر (مانند قانون‌گذاران[1]) را پیش از قرارداد جهت تعیین الزامات کارفرما برای متناسب‌سازی این استاندارد ملی برای پروژه را درگیر کند. به‌منظور تعیین این الزامات کارفرما باید تأثیر متناسب‌سازی الزامات بر فرایندهای پذیرفته‌شده سازمانی تأمین‌کننده را مدنظر قرار دهد. کارفرما باید الزامات متناسب‌سازی را در قرارداد گنجانده و یا به آن‌ها ارجاع دهد. ۶_۱_۱_۳_۴_۲ کارفرما باید قراردادی را با تأمین‌کننده آماده کرده و	۶_۱_۲_۳_۳ قرارداد توافق. این فعالیت شامل وظایف زیر است: ۶_۱_۲_۳_۳_۱ تأمین‌کننده باید برای تأمین محصول یا خدمت نرم‌افزاری با انجام مذاکره، وارد یک قرارداد با کارفرما شود. ۶_۱_۲_۳_۳_۲ ممکن است تأمین‌کننده به‌عنوان بخشی از سازوکار کنترل تغییر، تقاضای تغییراتی در قرارداد را کند.

1-Requlators

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
داده‌های فنی و مالکیت معنوی در توافق‌نامه ذکر می‌شود .هنگامی‌که کارفرما شرایط پیشنهادی تأمین‌کننده که در توافق‌نامه درج می‌شود را بپذیرد ، مذاکرات خاتمه می‌یابد. ۲) مبادله توافق‌نامه با تأمین‌کننده	زمان‌بندی‌های پرداخت مورد پذیرش‌اند. همچنین تأیید می‌کند که طرفین مبنایی برای اجرای توافق‌نامه به صورتی که عاری از مخاطرات غیرضروری باشد، پی‌ریزی می‌کنند. در توافق‌نامه یا طرح‌های پروژه، تأمین‌کننده باید مدل چرخه حیات متناسب با دامنه، اندازه و پیچیدگی پروژه را تعریف یا انتخاب کند. ایده‌آل آن است که این اقدام با استفاده از مدل چرخه حیاتی که در سطح سازمان تعریف شده، انجام شود. ۲) مبادله توافق‌نامه با کارفرما. .	مورد مذاکره قرار دهد. این قرارداد باید الزامات اکتساب شامل هزینه و زمان‌بندی تحویل محصول یا خدمت نرم‌افزاری را پوشش دهد. قرارداد باید حقوق اختصاصی استفاده، مالکیت، ضمانت و گواهی مرتبط با محصولات نرم‌افزاری آماده قابل‌استفاده مجدد را در نظر بگیرد. ۶_۱_۱_۳_۴_۳ هنگامی‌که قرارداد در جریان است، کارفرما باید تغییرات اعمال‌شده در فرایند از طریق مذاکره را به‌عنوان بخشی از سازوکار کنترل تغییر، کنترل کند. یادآوری ۱ _ کارفرما تعیین می‌کند که کدام‌یک از اصطلاحات «قرارداد» یا «توافقنامه» در هنگام به‌کارگیری این استاندارد ملی استفاده شوند. یادآوری ۲_ توصیه می‌شود توافق میان کارفرما و تأمین‌کننده به‌صورت شفاف انتظارات، مسئولیت‌ها و تعهدات طرفین را بیان کند. یادآوری ۳_ سازوکار کنترل تغییرات قرارداد باید نقش‌های مدیریت تغییر، سطح رسمیت درخواست‌های پیشنهاد تغییر و مذاکرات مجدد و ارتباطات با ذینفعانی که تحت تأثیر تغییرات قرار گرفته‌اند را پوشش دهد.	

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
		پیوست اطلاعاتی و شامل فرایند مدیریت تغییر یک قرارداد نمونه که می‌تواند در به‌کارگیری از این بند استفاده شود.	
ت) پایش توافق‌نامه. این فعالیت شامل کارهای زیر می‌شود: ۱) ارزیابی اجرای توافق‌نامه. یادآوری این ارزیابی شامل تأیید این‌که همه‌ی اشخاص، مسؤولیت‌های خود را مطابق با توافقنامه به انجام برسانند، است .هزینه‌های پیش‌بینی‌شده و مخاطرات عملکرد و زمان‌بندی پایش می‌شوند و تأثیر دستاوردهای نامطلوب بر روی سازمان، به‌طور مرتب ارزشیابی می‌شود .هرگونه انحراف از شرایط توافق‌نامه ، برحسب ضرورت ، مورد مذاکره قرار می‌گیرد. ۲) فراهم آوردن داده‌های موردنیاز تأمین‌کننده و حل کردن به‌موقع موضوعات.	ت) اجرای توافق‌نامه. این فعالیت شامل کارهای زیر می‌شود: ۱) اجرای توافق‌نامه مطابق با طرح‌های از پیش تعیین‌شده‌ی تأمین‌کننده و در انطباق با توافق‌نامه. یادآوری ۱- تأمین‌کننده ممکن است فرآیندهای کارفرما را قبول کرده یا با استفاده از آن‌ها موافقت کند. یادآوری ۲- ارتباط با کارفرما در طول اجرای توافق‌نامه حفظ می‌شود. ۲) ارزیابی اجرای توافق‌نامه. یادآوری مخاطرات از پیش تعیین‌شده‌ی مرتبط با هزینه، عملکرد و زمان‌بندی پایش می‌شوند و در صورت نیاز به اطلاع کارفرما رسانده می‌شود. اثر دستاوردهای نامطلوب بر سازمان مورد ارزیابی قرار می‌گیرد.	۶_۱_۱_۳_۵ پایش توافق. این فعالیت شامل وظایف زیر است: ۶_۱_۱_۳_۵_۱ کارفرما باید فعالیت‌های تأمین‌کننده را در انطباق با یک فرایند بازنگری نرم‌افزار (زیربند ۷_۲_۶) و فرایند ممیزی نرم‌افزار (۷_۲_۷) پایش کند. توصیه می‌شود در صورت نیاز کارفرما پایش را با فرایندهای درستی‌سنجی (زیربند ۷_۲_۴) و اعتبارسنجی (زیربند ۷_۲_۵) تکمیل کند. ۶_۱_۱_۳_۵_۲ کارفرما باید با تأمین‌کننده در مورد فراهم کردن تمام اطلاعات ضروری در مدت زمان مناسب و حل موارد در حال انتظار همکاری کند.	۶_۱_۱_۳_۵ اجرای قرارداد. این فعالیت شامل وظایف زیر است: ۶_۱_۲_۳_۴_۱ تأمین‌کننده باید الزامات کارفرما را به‌منظور تعریف چارچوبی برای مدیریت و تضمین پروژه و تضمین کیفیت محصولات و خدمات نرم‌افزاری تحویل‌شدنی مورد بازنگری قرار دهد. ۶_۱_۲_۳_۴_۲ درصورتی‌که در قرارداد تصریح نشده باشد، تأمین‌کننده باید یک مدل چرخه حیات را در تناسب با محدوده، اندازه و پیچیدگی پروژه تعریف یا انتخاب کند. مدل چرخه حیات بیان‌شده باید شامل مراحل و هدف و خروجی هر مرحله باشد. فرایندها، فعالیت‌ها و وظایف این استاندارد ملی باید انتخاب شده و به مدل چرخه حیات نگاشت شوند. یادآوری در حالت ایده‌آل، این کار با استفاده از یک مدل چرخه حیات تعریف‌شده در سطح سازمان انجام می‌شود. ۶_۱_۲_۳_۴_۳ تأمین‌کننده باید الزاماتی برای برنامه‌های مدیریت و تضمین پروژه و برای تضمین کیفیت اقلام تحویلی

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
			محصول یا خدمت نرم‌افزاری ایجاد کند. الزامات برنامه‌ها بهتر است شامل نیازهای منبع و مشارکت کارفرما باشد. ۶_۱_۲_۳_۴_۴ پس از ایجاد الزامات برنامه‌ریزی تأمین‌کننده باید گزینه‌های توسعه محصول نرم‌افزاری یا ارائه خدمت نرم‌افزاری را با به‌کارگیری تحلیل مخاطرات مربوط به هر گزینه در نظر بگیرد. گزینه‌ها شامل موارد زیر هستند: الف) توسعه محصول نرم‌افزاری یا ارائه خدمت نرم‌افزاری با استفاده منابع داخلی. ب) توسعه محصول نرم‌افزاری یا ارائه خدمت نرم‌افزاری از طریق قرارداد فرعی پ) تهیه محصولات نرم‌افزاری آماده از منابع داخلی یا خارجی. ت) ترکیبی از بندهای الف، ب و ج بالا. ۶ـ۱ـ۲ـ۳ـ۴ـ۵ تأمین‌کننده باید برنامه(های) مدیریت پروژه را بر مبنای الزامات برنامه‌ریزی و گزینه‌های انتخاب‌شده در بند ۶ـ۱ـ۲ـ۳ـ۴ـ۴ توسعه دهد. یادآوری ـ مواردی که باید در برنامه بیان‌شده لحاظ شوند شامل موارد زیر بوده اما به این موارد محدود نمی‌شود: الف) ساختار سازمانی پروژه و اختیار و مسئولیت هر یک از واحدهای سازمانی شامل سازمان‌های خارجی.

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
			ب) محیط مهندسی (برای توسعه، عملیات، با نگهداشت در صورت کاربردپذیری) شامل محیط آزمونُ کتابخانه، تجهیزات، تسهیلات، استانداردها، روش‌های اجرایی و ابزار. پ) ساختار شکست کار فرایندها فعالیت‌های چرخه حیات، شامل محصولات نرم‌افزاری، خدمات نرم‌افزاری موارد تحویلی برای انجام به همراه بودجه، نیروی کار، منابع فیزیکی، اندازه نرم‌افزار و برنامه‌های زمان‌بندی مربوط به وظایف. ت) مدیریت کیفیت ویژگی‌های محصول یا خدمت نرم‌افزاری. ممکن است برنامه‌های جداگانه‌ای برای کیفیت توسعه داده شوند. ث) مدیریت امنیت و دیگر الزامات حیاتی محصولات یا خدمات نرم‌افزاری. ممکن است برنامه‌های جداگانه‌ای برای امنیت توسعه داده شوند. ج) مدیریت پیمانکاران فرعی شامل انتخاب پیمانکار فرعی و مشارکت میان پیمانکار فرعی و کارفرما در صورت وجود چنین مشارکتی. چ) تضمین کیفیت (زیربند ۷_۲_۳ را مشاهده نمایید) ح) درستی‌سنجی (زیربند ۷_۲_۴ را مشاهده نمایید) و اعتبارسنجی (زیربند ۷_۲_۵

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
			را مشاهده نمایید) شامل رویکرد واسطه‌گری با عامل درستی‌سنجی و اعتبارسنجی درصورتی‌که مشخص شده باشد. خ) مشارکت با کارفرما؛ که از طریق روش‌هایی مانند بازنگری‌ها (زیربند ۷_۲_۶ را مشاهده نمایید) ممیزی‌ها (زیربند ۷_۲_۶ را مشاهده نمایید)، ملاقات غیررسمی، گزارشگری، تغییرات، پیاده‌سازی، تأیید، پذیرش و دسترسی به تسهیلات صورت می‌گیرد. د) مشارکت با کارفرما؛ که از طریق روش‌هایی مانند فعالیت‌های تنظیم الزامات، نمایش و ارزیابی نمونه‌ها صورت می‌گیرد. ذ) مدیریت مخاطرات؛ که مدیریت محدوده‌هایی از پروژه است که شامل مخاطرات بالقوه فنی، هزینه یا زمان‌بندی است. ر) سیاست امنیت[1]؛ که مدیریت قواعدی برای دانستن در حد نیاز و دسترسی به اطلاعات در هر یک از سطوح سازمانی پروژه است. ز) تأیید موردنیاز از طریق ابزارهایی مانند مقررات، گواهی‌های لازم، حقوق اختصاصی استفاده، مالکیت، ضمانت و مجوزدهی.

1- Security policy

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
			س) ابزارهایی برای زمان‌بندی، ردگیری و گزارشگری. ش) آموزش کارکنان (زیربند ۶_۲_۴ را مشاهده نمایید.) ۶_۱_۲_۳_۴_۶ تأمین‌کننده باید برنامه(های) مدیریت پروژه توسعه‌داده‌شده تحت بند ۶_۱_۲_۳_۴_۵ را پیاده‌سازی و اجرا کند. ۶_۱_۲_۳_۴_۷ تأمین‌کننده باید: الف) محصول نرم‌افزاری را در انطباق با فرایندهای فنی توسعه دهد (زیربند ۶_۴) ب) محصول نرم‌افزاری را در انطباق با فرایند عملیات نرم‌افزار عملیاتی کند (زیربند ۶_۴_۹) ج) محصول نرم‌افزاری را در انطباق با فرایند نگهداشت نرم‌افزار نگهداری کند (زیربند ۶_۴_۱۰) ۶_۱_۲_۳_۴_۸ تأمین‌کننده باید پیشرفت و کیفیت محصولات و خدمات نرم‌افزاری پروژه را در سراسر چرخه حیات قراردادشده پایش کند. این کار باید یک وظیفه ادامه‌دار تکراری باشد که برای موارد زیر ارائه شود: الف) پایش پیشرفت کارایی فنی، هزینه و برنامه زمان‌بندی و گزارشگری وضعیت پروژه. ب) شناسایی، ضبط، تحلیل و حل مشکل. ۶_۱_۲_۳_۴_۹ تأمین‌کننده

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
			باید پیمانکاران فرعی را منطبق با فرایند اکتساب مدیریت و کنترل کند (زیربند ۶_۱_۱). تأمین‌کننده باید تمام الزامات ضروری را برای تضمین این‌که تمام محصول یا خدمت نرم‌افزاری تحویل‌شده به کارفرما منطبق با الزامات پیمانکار اصلی توسعه یا انجام‌شده است، به پایین‌دستی‌ها منتقل کند. ۶_۱_۲_۳_۴_۱۱ تأمین‌کننده مطابق با قرارداد و برنامه‌های پروژه با دیگر اشخاص حاضر در پروژه ارتباط برقرار کند. ۶_۱_۲_۳_۴_۱۲ تأمین‌کننده باید فعالیت‌ها، روابط و ارتباطات بازنگری قرارداد را با کارفرما هماهنگ کند. ۶_۱_۲_۳_۴_۱۳ تأمین‌کننده باید جلسات غیررسمی، بازنگری پذیرش، آزمون پذیرش، بازنگری‌های مشترک و ممیزی‌ها را مطابق با قرارداد یا برنامه‌های پروژه با کارفرما انجام دهد. ۶_۱_۲_۳_۴_۱۴ توصیه می‌شود تأمین‌کننده درستی‌سنجی و اعتبارسنجی را در انطباق با زیربندهای ۷_۲_۴ و ۷_۲_۵ به‌منظور نمایش این‌که محصولات و خدمات نرم‌افزاری و فرایندها به‌صورت کامل الزامات موردنظر

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
			را برآورده می‌کنند، انجام دهد. ۶_۱_۲_۳_۴_۱۵ تأمین‌کننده باید گزارش‌های ارزیابی، بازنگری‌ها، ممیزی‌ها، آزمون و حل مشکلات را همان‌گونه که در قرارداد مشخص شده است، در اختیار کارفرما قرار دهد. ۶_۱_۲_۳_۴_۱۶ تأمین‌کننده باید دسترسی به تسهیلات تأمین‌کننده و پیمانکار را برای بازنگری محصولات یا خدمات نرم‌افزاری همان‌گونه که در قرارداد و برنامه‌های پروژه مشخص‌شده است، برای کارفرما فراهم کند. ۶_۱_۲_۳_۴_۱۷تأمین‌کننده باید فعالیت‌های تضمین کیفیت را مطابق را زیربند ۷_۲_۳ انجام دهد.
ث) پذیرش محصول یا خدمت .این فعالیت شامل کارهای زیر می‌شود: ۱) تأیید این‌که محصول یا خدمت تحویل‌داده‌شده منطبق با توافق‌نامه است. یادآوری استثنائاتی که در طول اجرای توافق‌نامه یا ضمن تحویل محصول یا خدمت حادث می‌شوند مطابق رویه‌های تمهید شده در توافقنامه حل‌وفصل می‌شوند.	ث) تحویل محصول یا خدمت و پشتیبانی از آن. این فعالیت شامل کارهای زیر می‌شود: ۱) تحویل محصول یا خدمت مطابق با معیارهای توافق‌نامه. ۲) ارائه‌ی کمک به کارفرما در راستای پشتیبانی از سامانه یا خدمت تحویل داده‌شده و براساس معیارهای توافق‌نامه.	۶_۱_۱_۳_۶ پذیرش کارفرما. این فعالیت شامل وظایف زیر است: ۶_۱_۱_۳_۶_۱ توصیه می‌شود کارفرما مطابق با راهبر و معیارهای تعریف‌شده پذیرش، برای پذیرش آماده شود. بهتر است آماده‌سازی موارد آزمون، داده‌های آزمایشی، روش‌های اجرایی آزمون و محیط آزمون گنجانده شوند. میزان مشارکت تأمین‌کننده باید تعریف شود. ۶_۱_۱_۳_۶_۲ کارفرما	۶_۱_۲_۳_۵ تحویل محصول /خدمت. این فعالیت شامل وظایف زیر است: ۶_۱_۲_۳_۵_۱ تأمین‌کننده باید محصول یا خدمت نرم‌افزاری را همان‌گونه که در قرارداد مشخص شده است تحویل دهد. یادآوری_ هنگامی‌که در توافقنامه الزام شده باشد، بهتر است تأمین‌کننده محصول را مطابق با الزامات ایجادشده نصب کند. ۶_۱_۲_۳_۵_۲ تأمین‌کننده باید مطابق با قرارداد کمک‌های

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
		باید بازنگری پذیرش و آزمون پذیرش مربوط به محصولات و خدمات نرم‌افزاری تحویل‌شدنی انجام داده و باید این موارد را زمانی از تأمین‌کننده قبول کند که تمامی شرایط پذیرش برآورده شده باشد. رویه پذیرش بهتر است با مقررات بند ۶_۱_۱_۳_۱_۹ مطابقت داشته باشد. ۶_۱_۱_۳_۶_۳ پس از پذیرش، توصیه می‌شود کارفرما مسئولیت مدیریت پیکربندی محصول نرم‌افزاری تحویل‌شده را عهده‌دار شود (زیربند ۷_۲_۲ را مشاهده نمایید). یادآوری_ ممکن است کارفرما مطابق با دستورالعمل‌های تعریف‌شده توسط تأمین‌کننده، محصول نرم‌افزاری را نصب کرده و یا خدمت نرم‌افزاری را اجرا کند.	لازم در مورد پشتیبانی محصول یا خدمت نرم‌افزاری تحویل‌شده را ارائه دهد.
۲) انجام پرداخت‌ها یا انجام سایر ملاحظات توافق شده با تأمین‌کننده محصول یا خدمت که برای خاتمه‌ی توافق‌نامه ضروری است.	ج -خاتمه‌ی توافق‌نامه. این فعالیت شامل کارهای زیر می‌شود: ۱) پذیرش و تأیید پرداخت‌ها یا سایر ملاحظات توافق شده. ۲) انتقال مسؤولیت محصول یا خدمت به کارفرما یا شخص دیگر ، بر مبنای آنچه در توافق‌نامه تصریح	۶_۱_۱_۳_۷ بستن. این فعالیت شامل وظایف زیر است: ۶_۱_۱_۳_۷_۱ کارفرما باید پرداخت پول یا دیگر موارد به تأمین‌کننده را جهت محصول یا خدمت ارائه‌شده انجام دهد. یادآوری ۱ _ هنگامی‌که محصول یا خدمت تأمین‌شده	۶_۱_۲_۳_۶ بستن. این فعالیت شامل وظایف زیر است: ۶_۱_۲_۳_۶_۱ تأمین‌کننده باید پرداخت پول یا دیگر موارد توافق‌شده را تأیید کند. ۶_۱_۲_۳_۶_۲ تأمین‌کننده باید مسئولیت محصول یا خدمت را به کارفرما یا شخص دیگری به صورتی که در توافقنامه برای بستن توافق

فرایند اکتساب سامانه‌ها (15288)	فرایند تأمین سامانه‌ها (15288)	فرایند اکتساب نرم‌افزار (12207)	فرایند تأمین نرم‌افزار (12207)
	شده است، به‌منظور خاتمه‌ی آن.	شرایط توافقنامه را برآورده کرده و موارد باز شناسایی‌شده به‌صورت رضایت‌بخش بسته شده‌اند کارفرما توافقنامه را با ارائه پرداخت یا موارد دیگر توافق‌شده و اعلام پایان توافق، پایان می‌دهد. یادآوری ۲_ ممکن است یک محصول یا خدمت به‌صورت افزایشی تأمین‌شده و پرداخت یا دیگر موارد توافق‌شده ممکن است در افزایش‌ها فراهم شوند.	راهنمایی شده است، انتقال دهد. یادآوری_ توافقنامه باید شرایط و اختیارات لازم برای شروع بستن پروژه را پوشش دهد.

پیوست ب

(اطلاعاتی)

نگاشت بند ۶ به استاندارد ISO/IEC 27002

جدول ب ـ۱ـ مخاطرات نمونه امنیت اطلاعات برای اکتساب خدمات

بند یا زیربند ISO/IEC 27036-3	بند یا زیربند ISO/IEC 27002
۶. امنیت زنجیره تأمین ICT در فرایندهای چرخه حیات	فرایندهای منفرد برای نگاشت‌های خاص را مشاهده نمایید
۶-۱فرایندهای توافق	۵. خط‌مشی امنیتی ۶. سازمان امنیت اطلاعات ۱۵. روابط تأمین‌کننده ۱۸. انطباق
۶-۱-۱فرایندهای اکتساب	به نگاشت ۶_۱ مراجعه کنید
۶-۱-۲فرایند توافق	به نگاشت ۶_۱ مراجعه کنید
۶-۲ فرایندهای توانمندساز پروژه سازمانی	فرایندهای منفرد برای نگاشت‌های خاص را مشاهده نمایید
۶-۲-۱ فرایند مدیریت مدل چرخه حیات	هیچ‌کدام
۶-۲-۲ فرایند مدیریت زیرساخت	۸. مدیریت دارایی ۹. کنترل دسترسی ۱۰. محرمانگی ۱۱. امنیت فیزیکی و محیطی ۱۲. امنیت عملیات ۱۳. امنیت ارتباطات ۱۶. مدیریت وقایع امنیت اطلاعات ۱۷. جنبه‌های امنیت اطلاعات مدیریت استمرار کسب‌وکار
۶-۲-۳ فرایند مدیریت سبد پروژه	هیچ‌کدام
۶-۲-۴ فرایند مدیریت منابع انسانی	۷. امنیت منابع انسانی
۶-۲-۵ فرایند مدیریت کیفیت	۱۴_۲ امنیت فرایندهای توسعه و پشتیبانی ۱۴_۳ داده آزمایشی
۶-۳ فرایندهای پروژه	فرایندهای منفرد برای نگاشت‌های خاص را مشاهده نمایید.
۶-۳-۱ فرایند طرح‌ریزی پروژه	هیچ‌کدام
۶-۳-۲ فرایند ارزیابی و کنترل پروژه	هیچ‌کدام
۶-۳-۳ فرایند مدیریت تصمیم	هیچ‌کدام
۶-۳-۴ فرایند مدیریت مخاطرات	استاندارد ملی ۲۷۰۰۵
۶-۳-۵ فرایند مدیریت پیکربندی	۱۲_۱_۲ مدیریت تغییر

بند یا زیربند ISO/IEC 27036-3	بند یا زیربند ISO/IEC 27002
	۱۴_۲_۲ روش‌های اجرایی کنترل تغییر سامانه
۶-۳-۶ فرایند مدیریت اطلاعات	۸_۲ رده‌بندی اطلاعات ۹_۱ کنترل دسترسی الزامات کسب‌وکار ۱۰ محرمانگی ۱۲_۳ نسخه پشتیبان ۱۳_۲_۱ روش‌های اجرایی و خط‌مشی‌های انتقال اطلاعات
۶-۳-۷ فرایند سنجش	ISO/IEC 27004
۶-۴ فرایندهای فنی	فرایندهای منفرد برای نگاشت‌های خاص را مشاهده نمایید.
۶-۴-۱ فرایند تعریف الزامات ذینفع	۱۴_۱ الزامات امنیتی برای سامانه‌های اطلاعاتی
۶-۴-۲ فرایند تحلیل الزامات	۱۴_۱ الزامات امنیتی برای سامانه‌های اطلاعاتی
۶-۴-۳ فرایند طراحی معمارانه	هیچ‌کدام
۶-۴-۴ فرایند پیاده‌سازی	۱۴_۲ امنیت فرایندهای توسعه و پشتیبانی
۶-۴-۵ فرایند یکپارچه‌سازی	۱۴_۲ امنیت فرایندهای توسعه و پشتیبانی
۶-۴-۶ فرایند درستی‌سنجی	۱۴_۲ امنیت فرایندهای توسعه و پشتیبانی ۱۴_۳ داده آزمایشی
٦-٤-٦٦-۴-۷ فرایند انتقال	۱۴_۲_۸ آزمون امنیت سامانه
٦-٤-٦٧-۴-۸ فرایند اعتبارسنجی	۱۴_۲ امنیت فرایندهای توسعه و پشتیبانی ۱۴_۳ داده آزمایشی
٦-٤-٦٨-۴-۹ فرایند عملیات	۸. مدیریت دارایی ۹. کنترل دسترسی ۱۰. محرمانگی ۱۲. امنیت عملیات ۱۳. امنیت ارتباطات ۱۶. مدیریت رخداد امنیت اطلاعات ۱۷. جنبه‌های امنیت اطلاعات مدیریت استمرار کسب‌وکار ۱۸. انطباق
٦-٤-٦٩-۴-۱۰ فرایند نگهداشت	۸_۳ اداره رسانه ۱۳. امنیت ارتباطات ۱۷. جنبه‌های امنیت اطلاعات مدیریت استمرار کسب‌وکار
٦-٤-٦١٠-۴-۱۱ فرایند امحا	۸. مدیریت دارایی ۱۳_۲ انتقال اطلاعات

کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۱۵۰۲۶: سال ۱۳۹۲، مهندسی سامانه و نرم‌افزار- تضمین سامانه‌ها و نرم‌افزار قسمت ۲- مورد تضمین

[۲] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات – الزامات

[۳] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات – آیین کار مدیریت امنیت اطلاعات

[۴] استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت مخاطرات امنیت اطلاعات

[۵] استاندارد ملی ایران شماره ۲۷۰۰۷: سال ۱۳۹۱، فناوری اطلاعات – فنون امنیتی – راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات

[۶] استاندارد ملی ایران شماره ۱۶۰۳۴: سال ۱۳۹۱، مهندسی سامانه ها و نرم افزار- فرایند های چرخه حیات سامانه

[7] ISO/IEC 12207, Systems and software engineering — Software life cycle processes

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

[9] ISO 28001, Security management systems for the supply chain — Best practices for implementing

[10] ISO/IEC 20000‑1, Information technology — Service management — Part 1: Service management system requirements

[11] Software Assurance Forum for Excellence in Code (SAFECode), The Software Supply Chain Integrity Framework, Defining Risks and Responsibilities for Securing Software in the Global Supply Chain, July 21, 2009

[12] SAFECode, Software Integrity Controls, An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain, June 14, 2010

[13] National Institute of Standards and Technology Interagency Report 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems, October 2012