INSO-ISO-IEC

27036-2

1st.Edition

2016

Identical with

ISO/IEC 27036-2:
2014

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران ایزو آی سی

۲۷۰۳۶-۲

چاپ اول

۱۳۹۵

فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط با تأمین‌کننده – قسمت ۲: الزامات

Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements

ICS: 35.040

سازمان ملی استاندارد ایران

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

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

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

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

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

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

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و کسب‌وکار است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تدارک می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها واسط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و الزامات خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، پیاده‌سازی بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، پیاده‌سازی استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط با تأمین‌کننده –قسمت ۲: الزامات»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی)	مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات
اعضاء: (اسامی به ترتیب حروف الفبا)	
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
دوست‌محمدی، وحید (کارشناسی ارشد مهندسی صنایع گرایش فناوری اطلاعات)	کارشناس مرکز مدیریت راهبردی افتا
محمدیان، بهزاد (فوق لیسانس مهندسی برق)	کارشناس مرکز مدیریت راهبردی افتا
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

ارجمند، مهدی
(کارشناسی ارشد مهندسی کامپیوتر)
پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

رادمهر، وحید
(کارشناسی مهندسی کامپیوتر)
پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

جوادزاده، غزاله
(کارشناسی ارشد مهندسی کامپیوتر)
پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

مغانی، مهدی
(فوق لیسانس ریاضی کاربردی)
کارشناس تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران

ویراستار:

قسمتی، سیمین
(کارشناسی ارشد مهندسی فناوری اطلاعات)
مشاور مرکز آپا دانشگاه تربیت مدرس

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط با تأمین‌کننده – قسمت ۲: الزامات» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است، در چهارصد و بیست و نهمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۰۲/۲۰ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به توصیف زیر است:

ISO/IEC 27036-2: 2014, Information Technology — Security Techniques — Information Security for Supplier Relationships— Part 2: Requirement

مقدمه

سازمان‌ها در سراسر جهان، برای اکتساب محصولات و خدمات با تأمین‌کنندگان کار می‌کنند. بسیاری از سازمان‌ها برای پوشش نیازهای متنوع کسب‌وکار، روابط زیادی مانند بهره‌برداری یا ساخت با تأمین‌کنندگان ایجاد می‌کنند. از طرق مقابل، تأمین‌کنندگان محصولات و خدمات را با کارفرمایان زیادی فراهم می‌کنند.

ممکن است، روابط بین کارفرمایان و تأمین‌کنندگان که به‌منظور اکتساب محصولا و خدمات مختلف ایجاد شده است، مخاطرات امنیت اطلاعات را برای هر دو طرف کارفرمایان و تأمین‌کنندگان ایجاد کند. این مخاطرات، با دسترسی متقابل به دارایی‌های طرف دیگر مانند اطلاعات و سامانه‌های اطلاعاتی، و همچنین در اثر تفاوت اهداف کسب‌وکار و رویکردهای امنیت اطلاعات، روی می‌دهد. این مخاطرات باید توسط هردوی کارفرمایان و تأمین کنندگان مدیریت شود.

استاندارد ملی ۲۷۰۳۶-۲:

الف) الزامات بنیادی امینت اطلاعات را برای تعریف، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداشت و بهبود روابط تأمین‌کننده و کارفرما مشخص می‌کند؛

ب) درک متقابل رویکرد طرف مقابل در مورد امنیت اطلاعات و تحمل‌پذیری در برابر مخاطرات امنیت اطلاعات را تسهیل می‌کند؛

پ) پیچیدگی مدیریت مخاطراتی که می‌تواند اثرات امنیت اطلاعاتی بر روابط تأمین‌کننده و کارفرما داشته باشد را منعکس می‌کند؛

ت) برای استفاده توسط هر سازمانی که قصد ارزیابی امنیت اطلاعات را در روابط با تأمین‌کننده یا کارفرما دارد، درنظر گرفته شده است.

ث) برای مقاصد اعطای گواهینامه در نظر گرفته نشده است؛

ت) برای استفاده به عنوان چند هدف تعریف‌شده امنیت اطلاعات با کاربست‌پذیری در یک رابطه با تأمین‌کننده و کارفرما در نظر گرفته شده است که مبنایی برای مقاصد حصول اطمینان است.

استاندارد ملی ایران شماره ۲۷۰۳۶-قسمت ۱ دیدکلی و مفاهیم مرتبط با امنیت اطلاعات در روابط با تأمین‌کننده را ارائه می‌کند.

استاندارد ملی ۲۷۰۳۶-قسمت ۳ راهنماهایی برای کارفرما و تأمین‌کننده برای مدیریت مخاطرات امنیت اطلاعات مخصوص زنجیره تأمین محصولات و خدمات فناوری اطلاعات و ارتباطات(ICT) ارائه می‌کند.

استاندارد ISO/IEC 27036-4 (منتشر خواهد شد) راهنماهایی را برای کارفرما و تأمین‌کننده به منظور مدیریت مخاطرات امنیت اطلاعات مخصوص خدمات ابری ارائه می‌کند.

یادآوری- کاربر این سند لازم است هریک از اَشکال بیان قیود (مانند «باید[1]»، «نباید[2]»، «توصیه می‌شود[3]» و «توصیه نمی‌شود[4]») را به عنوان الزاماتی که باید برآورده شود و یا توصیه‌هایی که در آن‌ها آزادی انتخاب وجود دارد، به درستی تفسیر کند.

1 - Shall
2 - Shall not
3 -Should
4 -Should not

فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط با تأمین‌کننده –

قسمت ۲: الزامات

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین الزامات بنیادی امنیت اطلاعات به‌منظور تعریف، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود روابط تأمین‌کننده[1] و کارفرما[2] است.

این الزامات، هرگونه تدارک یا تأمین محصولات و خدمات، مانند ساخت یا هم‌گذاری[3]، تدارک فرایند کسب‌وکار، مؤلفه‌های نرم‌افزاری و سخت‌افزاری، تدارک فرایند دانش، خدمات ساخت-بهره‌برداری-انتقال[4](BOT) و رایانش ابری[5] را پوشش می‌دهد.

این الزامات به‌منظور استفاده در تمام سازمان‌ها، فارغ از نوع، اندازه و طبیعت آن‌ها، در نظر گرفته شده است.

برای برآورده کردن این الزامات، سازمان باید از قبل تعدادی از فرایندهای بنیادی را به‌صورت داخلی پیاده‌سازی کند و یا آن‌که فعالانه برای چنین کاری طرح‌ریزی کرده باشد. این فرایندها شامل موارد زیر هستند اما به این موارد محدود نمی‌شود: حاکمیت، مدیریت کسب‌وکار، مدیریت مخاطرات، مدیریت منابع عملیاتی و انسانی و امنیت اطلاعات.

۲ مراجع الزامی

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

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

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شمارهٔ ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی -سامانه‌های

1 - Supplier
2 - Acquirer
3 - Assembly
4 - Build-Operate-Transfer
5- Cloud computing

مدیریت امنیت اطلاعات مرور کلی و واژگان

۲-۲ استاندارد ملی ایران شماره ۲۷۰۳۶: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی -امنیت اطلاعات برای روابط تامین کننده -قسمت ۱- مرور کلی و مفاهیم

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف ارائه‌شده در استاندارد ISO/IEC 27000 و استاندارد ISO/IEC27036-1 به کار می‌رود.

۴ کوته‌نوشت‌ها

ASP	Application Service Provider	فراهم‌کننده خدمات برنامه کاربردی[1]
BCP	Business Continuity Plan	طرح تداوم کسب‌وکار
DBA	Database Administrator	راهبر پایگاه داده
ICT	Information and Communication Technology	فناوری اطلاعات و ارتباطات
ISMS	Information Security Management System	سامانه مدیریت امنیت اطلاعات
ITT	Invitation to Tender	دعوت به مناقصه
RFP	Request for Proposal	درخواست پیشنهاد
VoIP	Voice over Internet Protocol	صدا بر روی پروتکل اینترنت

۵ ساختار این استاندارد

بند ۶ الزامات بنیادی و سطح بالای امنیت اطلاعات که برای مدیریت روابط چند تأمین‌کننده کاربرد دارد را تعریف می‌کند. هریک از فرایندهای بند ۶ می‌تواند در روابط هر تأمین‌کننده در هر نقطه‌ای از چرخه

---

۱ - در فهرست واژگان مصوب فرهنگستان زبان و ادب فارسی، «رساننده خدمات کاربردی» ترجمه شده است.

حیات رابطه آن تأمین‌کننده اعمال شود.

ساختار این الزامات با توجه به فرایندهای چرخه حیات مشخص‌شده در ISO/IEC 15288 [۱] تنظیم شده است. این الزامات باید توسط کارفرما و تأمین‌کننده برای حصول اطمینان از توانایی این سازمان‌ها در مدیریت مخاطرات امنیت حاصل از روابط با تأمین‌کننده به‌کارگرفته شود.

یادآوری- بند ۶ تنها آن دسته از فرایندهای چرخه حیات ISO/IEC 15288 را که مرتبط با امنیت اطلاعات در روابط با تأمین‌کننده هستند، ارجاع می‌دهد.

بند ۷، الزامات بنیادی امنیت اطلاعات را تعریف می‌کند که در مورد رابطه کارفرما با تأمین‌کننده در زمینه یک نمونه رابطه با تأمین‌کننده منفرد کاربست‌پذیر است.

این الزامات با توجه به فرایندهای چرخه حیات روابط با تأمین‌کننده زیر سازمان‌دهی شده‌اند:

الف- فرایند طرح‌ریزی رابطه با تأمین‌کننده؛

ب- فرایند انتخاب تأمین‌کننده؛

پ- فرایند حصول توافق باتأمین‌کننده[1]؛

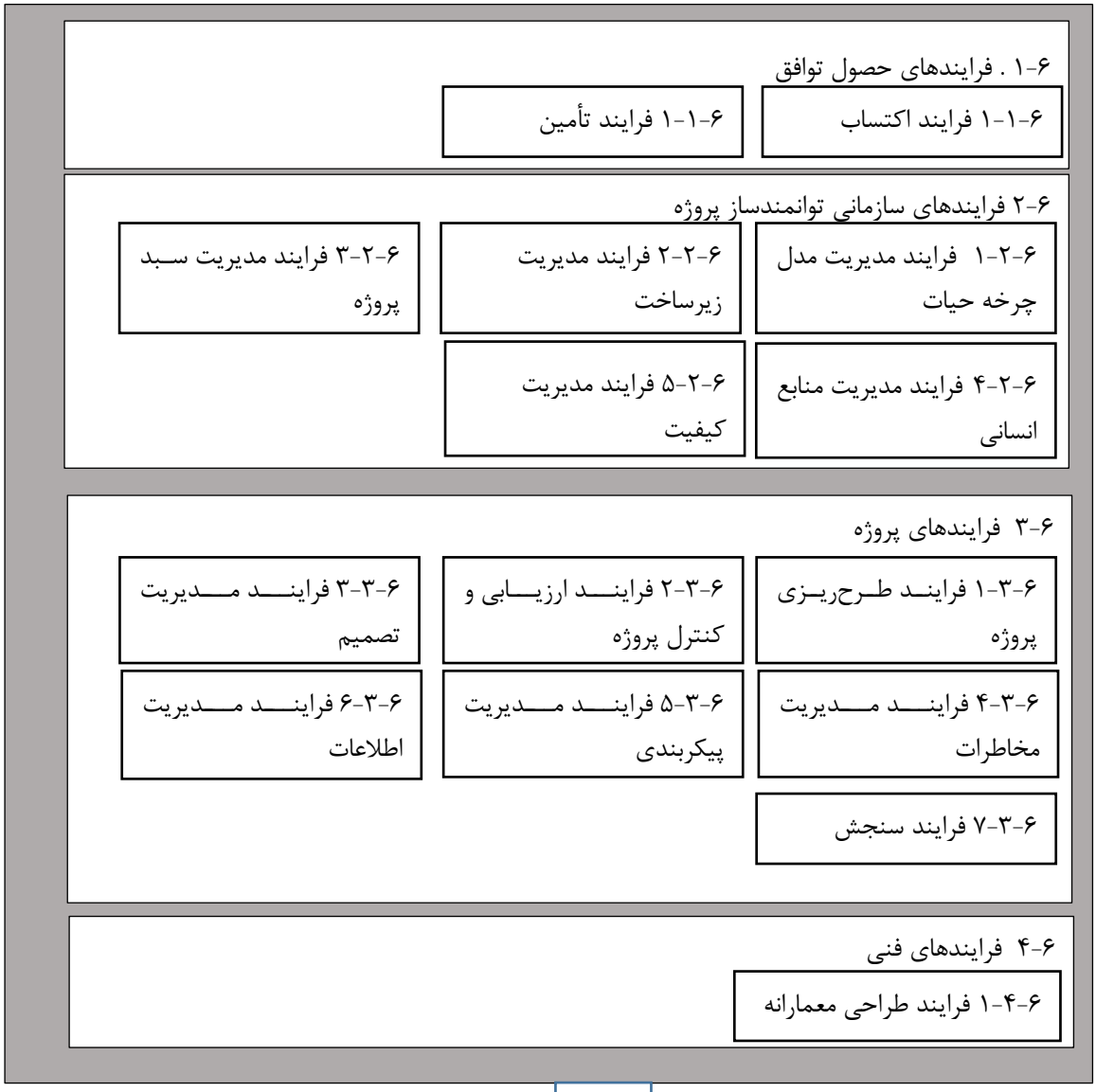
ت- فرایند مدیریت رابطه با تأمین‌کننده؛

ث- فرایند خاتمه رابطه با تأمین‌کننده؛

الزامات بند ۷ باید توسط کارفرما و تأمین‌کننده درگیر در رابطه با تأمین‌کننده رعایت شود تا اطمینان حاصل شود که این سازمان‌ها توانایی مدیریت مخاطرات امنیت اطلاعات مرتبط را دارا هستند.

شکل ۱ محدوده الزامات بنیادی امنیت اطلاعات در ارتباط با فرایندهای تعریف‌شده در بندهای ۶ و ۷ را توصیف می‌کند.

1 - Supplier relationship agreement process



شکل ۱- محدوده الزامات بنیادی امنیت اطلاعات تعریف‌شده در بندهای ۶ و ۷

متن بندهای ۶-۱ تا ۶-۴ و بندهای ۷-۱ تا ۷-۴ در جداولی ساختار یافته است که لازم است مانند زیر تفسیر شود:

کارفرما
متن مخصوص کارفرما

تأمین‌کننده
متن مخصوص تأمین‌کننده

کارفرما	**تأمین‌کننده**
متن مخصوص هر دو طرف کارفرما و تأمین‌کننده، مگر آن‌که به‌صورت صریح بیان شود.	
متن مخصوص کارفرما	متن مخصوص تأمین‌کننده

سه پیوست آگاهی‌دهنده وجود دارد:

پیوست الف، ارجاعات متقابل میان بندهای استاندارد ISO/IEC 15288 که مرتبط با روابط با تأمین‌کننده هستند و بندهای ISO/IEC 27036-2 را ارائه می‌کند.

پیوست ب، ارجاعات متقابل میان بندهای استاندارد ISO/IEC 27036-2 و آن دسته از کنترل‌های استاندارد ISO/IEC 27002 [۲] که مرتبط با روابط با تأمین‌کننده هستند را ارائه می‌کند.

پیوست پ، فهرستی از اهداف بیان‌شده در بندهای ۶ و ۷ برای کارفرما و تأمین‌کننده را ارائه می‌کند.

۶ امنیت اطلاعات در مدیریت رابطه با تأمین‌کننده

۶-۱ فرایندهای حصول توافق

سازمان‌ها می‌توانند در انواع روابط با تأمین‌کننده وارد شوند. روابط مناسب میان کارفرمایان و تأمین‌کنندگان با استفاده از توافقنامه‌هایی که نقش‌ها و مسئولیت‌های امنیت اطلاعات را با توجه به رابطه با تأمین‌کننده تعریف می‌کند، حاصل می‌شود.

فرایندهای حصول توافق زیر، تدارک یا تأمین محصول یا خدمت را از هر دو منظر راهبردی و امنیت اطلاعات پشتیبانی می‌کند.

الف- فرایند اکتساب؛

ب- فرایند تأمین.

۶-۱-۱ فرایند اکتساب

۶-۱-۱-۱ هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند اکتساب محقق شود.

کارفرما
الف- ایجاد راهبرد رابطه با تأمین‌کننده که: ۱- بر مبنای میزان تحمل مخاطرات امنیت اطلاعات کارفرما باشد؛ ۲- بنیان امنیت اطلاعات را برای استفاده در زمان طرح‌ریزی، آماده‌سازی، مدیریت و خاتمه تدارک محصول یا خدمت تعریف نماید.

۶-۱-۱-۲ فعالیت‌ها

کمینه فعالیت‌های زیر باید توسط کارفرما به‌منظور دستیابی به اهداف تعریف‌شده در بند ۶-۱-۱-۱ اجرا شود:

کارفرما
الف- تعریف، پیاده‌سازی، نگهداری و بهبود راهبرد رابطه با تأمین‌کننده شامل موارد زیر:

۱- انگیزه‌ها، نیازها و انتظارات مدیریت از تدارک محصولات یا خدمات؛

یادآوری- این بیانیه‌ها باید از منظر کسب‌وکار، عملیاتی، قانونی و مقراراتی[1] بیان شود.

۲- تعهد مدیریت به اختصاص منابع لازم؛

۳- چارچوبی برای مدیریت مخاطرات امنیتی برای استفاده در ارزیابی مخاطرات امنیت اطلاعات مربوط به تدارک محصول یا خدمت؛

یادآوری- بند ۶-۳-۴ الزامات امنیت اطلاعات مربوط به ایجاد چارچوب مدیریت مخاطرات امنیت اطلاعات را تعریف می‌کند.

۴- چارچوبی برای استفاده در هنگام تعریف الزامات امنیت اطلاعات در طول فرایند طرح‌ریزی رابطه با تأمین‌کننده؛

این چارچوب باید با رعایت راهنماها و قواعد امنیت اطلاعات، مانند خط‌مشی امنیت اطلاعات و رده‌بندی اطلاعات که توسط کارفرما ایجاد شده است، تعریف شود.

نیاز است، الزامات امنیت اطلاعات تعریف‌شده در این چارچوب، با در نظر گرفتن نوع و طبیعت محصول یا خدمت تدارک‌شده، برای هر نمونه از رابطه با تأمین‌کننده سفارشی‌سازی شود.

این چارچوب باید موارد زیر را نیز شامل شود:

i) روش‌هایی برای فراهم کردن شواهد پیروی از الزامات امنیت اطلاعات تعریف‌شده

ii) روش‌هایی به‌منظور اعتبارسنجی میزان پیروی تأمین‌کننده از الزامات امنیتی؛

iii) فرایندهایی برای به اشتراک گذاری اطلاعات درباره تغییرات ، رخدادها و دیگر رویدادهای امنیت اطلاعات میان کارفرما و تأمین‌کنندگان

۵-چارچوب معیارهای انتخاب تأمین‌کننده به‌منظور استفاده در زمان انتخاب تأمین‌کننده که شامل موارد زیر است:

i) روش‌هایی برای ارزیابی بلوغ امنیت اطلاعات که برای تأمین‌کننده الزامی است؛

عناصر زیر می‌تواند ازتأمین‌کننده برای ارزیابی بلوغ امنیت اطلاعات درخواست شود:

۱- عملکرد مرتبط با امنیت در گذشته

۲- شواهد مدیریت پیش‌بینانه امنیت اطلاعات(مانند دارا بودن گواهینامه ISO/IEC 27001 مرتبط با تأمین محصول یا خدمت-

1- Regulatory

۳- شواهد طرح‌های مستند و آزمون‌شده تداوم کسب‌وکار و تداوم فناوری اطلاعات و ارتباطات

ii) روش‌هایی برای استفاده به‌منظور ارزیابی شواهد ارائه‌شده توسط تأمین‌کننده بر مبنای الزامات تعریف‌شده امنیت اطلاعات

iii) روش‌هایی به‌منظور ارزیابی پذیرش موارد زیر توسط تأمین‌کننده:

۱- الزامات امنیت اطلاعات تعریف‌شده در طرح رابطه با تأمین‌کننده؛

۲- تعهد به پشتیبانی کارفرما در فعالیت‌های پایش و اعمال[1] انطباق با الزامات.

۳- انتقال تأمین محصول یا خدمتی که ممکن است قبلاً به‌وسیله کارفرما یا تأمین‌کننده دیگری ساخته یا بهره‌برداری شده باشد.

۴- خاتمه تأمین محصول یا خدمت.

iv) الزامات مختص به تأمین‌کننده، که توسط کارفرما مطابق با انتظارات کسب‌وکار، قانونی، مقرراتی، معماری، خط‌مشی‌ها و قراردادی تعریف شود. نمونه‌هایی از این الزامات مانند زیر است:

۱- قدرت مالی تأمین‌کننده برای توانایی تأمین محصول یا خدمت

۲- محل تأمین‌کننده که خدمت یا محصول از آنجا تأمین می‌شود به خصوص برای کاهش مخاطرات رخنه‌های قانونی و مقرراتی.

۶- الزامات سطح بالای امنیت اطلاعات برای استفاده در زمان تعریف موارد زیر:

i) طرح گذار برای انتقال محصول یا خدمت تدارک‌شده به تأمین‌کننده دیگر؛

ii) روش اجرایی مدیریت تغییرات امنیت اطلاعات؛

iii) روش اجرایی مدیریت رخدادهای امنیت اطلاعات؛

iv) طرح پایش و اعمال انطباق؛

v) طرح خاتمه به‌منظورخاتمه تدارک یک محصول یا خدمت.

ب- انتصاب فردی با مسئولیت ساماندهی جنبه‌های امنیت اطلاعات راهبرد رابطه با تأمین‌کننده و حصول اطمینان از اینکه فرد مذکور به‌صورت مناسب و منظم تحت آموزش قرار گرفته است.

پ- حصول اطمینان از اینکه راهبرد رابطه با تأمین‌کننده، کمینه یک‌بار در سال و همچنین در موارد وقوع تغییرات چشمگیر کسب‌وکار، قانونی، مقرراتی، معماری، خط‌مشی‌ها و قراردادی مورد بازنگری قرار

1 - Enforcement

می‌گیرد.

یادآوری- بهتر است راهبرد رابطه با تأمین‌کننده در زمان تدارک محصول یا خدمتی که می‌تواند به‌صورت چشمگیری بر کارفرما تأثیرگذار باشد نیز مورد بازنگری قرار گیرد.

۶-۱-۲ فرایند تأمین

۶-۱-۲-۱ هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند تأمین توسط تأمین‌کننده محقق شود:

تأمین‌کننده
الف- ایجاد راهبرد رابطه با کارفرما که: ۱- بر مبنای میزان تحمل مخاطرات امنیت اطلاعات توسط تأمین‌کننده باشد؛ ۲- بنیان امنیت اطلاعات را برای استفاده در زمان طرح‌ریزی، آماده‌سازی، مدیریت و خاتمه تأمین محصول یا خدمت تعریف نماید.

۶-۱-۲-۲ فعالیت‌ها

کمینه فعالیت‌های زیر باید توسط تأمین‌کننده به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۱-۲-۱ اجرا شود.

تأمین‌کننده
الف- تعریف، پیاده‌سازی، نگهداری و بهبود راهبرد رابطه کارفرما شامل موارد زیر: ۱- انگیزه‌ها، نیازها و انتظارات مدیریت از تأمین محصولات یا خدمات؛ **یادآوری**- این بیانیه‌ها باید از منظر کسب‌وکار، عملیاتی، قانونی و مقرراتی بیان شود. ۲- تعهد مدیریت به تخصیص[1] منابع لازم؛ ۳- چارچوبی برای مدیریت مخاطرات امنیتی برای ارزیابی مخاطرات امنیت اطلاعات مربوط به تأمین محصول یا خدمت **یادآوری**- بند ۶-۳-۴ الزامات امنیت اطلاعات مربوط به ایجاد چارچوب مدیریت مخاطرات امنیت اطلاعات را تعریف

1 - Allocate

می‌کند.

۴- چارچوبی برای مدیریت امنیت اطلاعات از طریق اقدامات زیر:

i) تعریف، پیاده‌سازی، نگهداری و بهبود مدیریت امنیت اطلاعات درونسازمان؛

یادآوری- ایجاد ISMS بر مبنای ISO/IEC 27001 می‌تواند برای حصول اطمینان از مدیریت کافی امنیت اطلاعات در سازمان و همچنین برای نمایش سطح مدیریت امنیت اطلاعات به کارفرما به کار رود.

ii) حصول اطمینان از اینکه الزامات امنیت اطلاعات بیان‌شده در اسناد مناقصه موجود کارفرما و توافقنامه‌های فی‌مابین به‌منظور اطمینان از انطباق امنیت اطلاعات تأمین‌کننده با آن‌ها شناسایی شده است؛

هر شکافی در این زمینه، به‌منظور بر آورده کردن الزامات امنیت اطلاعات کارفرما از توافقنامه‌های موجود با تأمین‌کننده، بررسی شود.

iii) تعریف فرایندی برای پذیرش، تفسیر، به‌کارگیری و سنجش الزامات امنیت اطلاعات کارفرما.

۵-روش‌هایی برای:

i) نمایش ظرفیت تأمین‌کننده در زمینه تأمین محصول یا خدمت با کیفیت قابل‌قبول؛

ii) فراهم کردن شواهدی مبنی بر رعایت الزامات امنیت اطلاعات تعریف‌شده توسط کارفرما.

۶- الزامات سطح بالای امنیت اطلاعات برای استفاده در زمان تعریف موارد زیر:

i) طرح گذار برای پشتیبانی از انتقال تأمین محصول یا خدمتی که قبلاً به‌وسیله کارفرما یا تأمین‌کننده دیگری ساخته یا بهره‌برداری شده است.

ii) روش اجرایی مدیریت تغییرات امنیت اطلاعات؛

iii) روش اجرایی مدیریت رخدادهای امنیت اطلاعات؛

iv) فرایندهایی در زمینه به اشتراک گذاشتن اطلاعات مربوط به تغییرات امنیت اطلاعات، رخدادها و دیگر رویدادهای مرتبط در میان تأمین‌کننده و کارفرما؛

v) فرایندهایی برای ساماندهی اقدامات اصلاحی؛

vi) طرح خاتمه به‌منظور خاتمه تأمین یک محصول یا خدمت.

ب- انتصاب فردی با مسئولیت ساماندهی جنبه‌های امنیت اطلاعات راهبرد رابطه کارفرما و حصول اطمینان از این که فرد مذکور به‌صورت مناسب و منظم تحت آموزش قرار گرفته است.

پ- حصول اطمینان از این که راهبرد رابطه کارفرما کمینه یک‌بار در سال و همچنین در موارد وقوع تغییرات چشمگیر کسب‌وکار، قانونی، مقرراتی، معماری، خط‌مشی و قراردادی مورد بازنگری قرار می‌گیرد.

یادآوری- بهتر است راهبرد رابطه کارفرما در زمان ایجاد رابطه با تأمین‌کننده‌ای که می‌تواند بر تأمین‌کننده تأثیر چشمگیری داشته باشد نیز مورد بازنگری قرار گیرد.

۶-۲ فرایندهای توانمندساز پروژه[1] سازمانی

فرایندهای توانمندساز پروژه سازمانی در ارتباط با حصول اطمینان از تخصیص منابع موردنیاز مانند منابع مالی است، که برای توانمند کردن پروژه در راستای برآورده کردن نیازها و انتظارات اشخاص ذینفع سازمان لازم هستند.

به خصوص، فرایندهای توانمندساز پروژه سازمانی زیر، از ایجاد محیطی که در آن روابط با تأمین‌کننده اجرا یا طرح‌ریزی شود، پشتیبانی می‌کنند:

الف- فرایند مدیریت مدل چرخه حیات؛

ب- فرایند مدیریت زیرساخت؛

پ- فرایند مدیریت سبد پروژه[2]؛

ت- فرایند مدیریت منابع انسانی؛

ث- فرایند مدیریت کیفیت.

۶-۲-۱ فرایند مدیریت مدل چرخه حیات

کارفرما	تأمین‌کننده
الف- کارفرما و تأمین‌کننده باید فرایند مدیریت مدل چرخه حیات را در زمان مدیریت امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند. **یادآوری**- هدف از این فرایند تعریف، نگهداری، و حصول اطمینان از دسترس‌پذیر بودن خط‌مشی‌ها، فرایندهای چرخه حیات، مدل‌های چرخه حیات، و روش‌های اجرایی برای استفاده توسط سامان است. هیچ‌گونه الزامات و توصیه‌های امنیت اطلاعات مشخصی برای لحاظ شدن توسط کارفرما و تأمین‌کننده در زمان ایجاد این فرایند وجود ندارد.	

1 - Project-enabling
2 - portfolio

۶-۲-۲ فرایند مدیریت زیرساخت

۶-۲-۲-۱هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند مدیریت زیرساخت توسط هریک از سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- فراهم کردن زیرساخت توانمندساز به‌منظور پشتیبانی سازمان در زمینه مدیریت زیرساخت امنیت اطلاعات در روابط با تأمین‌کننده.	

۶-۲-۲-۲ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۲-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- تعریف، پیاده‌سازی، نگهداری و بهبود قابلیت‌های فیزیکی و منطقی زیرساخت امنیت به‌منظور محافظت از دارایی‌های کارفرما یا تأمین‌کننده، مانند اطلاعات و سامانه‌های اطلاعاتی؛ و ب- تعریف، پیاده‌سازی، نگهداری و بهبود تمهیدات اقتضایی به‌منظور حصول اطمینان از این که تدارک یا تأمین محصول یا خدمت موردنظر می‌تواند در صورت وقوع اختلال به دلایل طبیعی یا انسانی ادامه یابد. این تمهیدات باید بر مبنای ارزیابی مخاطرات امنیت اطلاعات و طرح‌های برخورد با آن‌ها که از تدارک یا تأمین محصول یا خدمتی حاصل شده‌اند باشد و شامل موارد زیر باشد: ۱- فراهم کردن تسهیلات جایگزین امن برای تداوم تأمین محصول یا خدمت؛ ۲- سپردن اطلاعات و فناوری‌های مربوط به آن‌ها مانند کد منبع برنامه کاربردی و کلیدهای رمزنگاشتی[1] به طرف سوم[2] مطمئن؛ ۳- تمهیدات بازیابی به‌منظور حصول اطمینان از دسترس‌پذیری مداوم اطلاعات ذخیره‌شده در محل پیمانکار فرعی[1]؛ و	

1 - Cryptographic
2 - Third party

یادآوری- این تمهیدات تنها باید زمانی در نظر گرفته شود که تأمین‌کننده خدماتی را برای کارفرما تأمین می‌کند.

۴- هم‌راستایی با قیدهای تداوم کسب‌وکار بیان‌شده توسط کارفرما یا تأمین‌کننده.

یادآوری- استانداردهای بین‌المللی زیر الزامات و راهنماهایی برای تمهیدات اقتضایی فراهم می‌کنند:

۱- ISO/IEC 27031 [۳]

۲- ISO 22313 [۷]

۳- ISO 22301 [۸]

۶-۲-۳ فرایند مدیریت سبد پروژه[2]

۶-۲-۳-۱ هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند مدیریت سبد پروژه توسط هریک از سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- ایجاد فرایندی برای در نظر گرفتن امنیت اطلاعات و استلزام‌ها و وابستگی‌های کلی کسب‌وکار مربوط به هر پروژه، برای آن دسته از پروژه‌هایی که تأمین‌کنندگان یا کارفرمایان در آن درگیر هستند.	

۶-۲-۳-۲ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۳-۱-۲-۶۱-۳-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- تعریف، پیاده‌سازی، نگهداری و بهبود فرایندی برای شناسایی و طبقه‌بندی تأمین‌کنندگان یا کارفرمایان بر مبنای حساسیت اطلاعاتی که با آن‌ها به اشتراک گذاشته شده است و سطح دسترسی آن‌ها به دارایی‌های کارفرما یا تأمین‌کننده، مانند اطلاعات یا سامانه‌های اطلاعاتی؛ **یادآوری**- ممکن است تأمین‌کننده‌ای که دسترسی بسیار محدودی به دارایی‌های کارفرما مانند اطلاعات و سامانه‌های	

1 - Subcontractor

2 - Project portfolio

اطلاعاتی دارد، به‌عنوان غیر بحرانی طبقه‌بندی شود، درحالی‌که تأمین‌کننده‌ای که توسعه سامانه‌های بحرانی کسب‌وکار را بر عهده دارد به‌عنوان بحرانی طبقه‌بندی شود.	
ب-تعریف، پیاده سازی، نگهداری و بهبود فرایندی برای حصول اطمینان از این که ملاحظات امنیت اطلاعات در ارزیابی عملکرد تأمین‌کننده به‌عنوان قسمتی از هر پروژه گنجانده شده‌اند؛ و	
ج- حصول اطمینان از این که تکمیل پروژه‌ای که کارفرما یا تأمین‌کننده‌ای در آن دخالت دارند، شامل فعالیت‌های امنیت اطلاعاتی است که در طرح خاتمه مستند شده است.	

۶-۲-۴ فرایند مدیریت منابع انسانی

۶-۲-۴-۱هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند مدیریت منابع انسانی توسط هریک از سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- حصول اطمینان از این که کارفرما و تأمین‌کننده دارای نیروهای انسانی هستند که دارای شایستگی‌های منطبق با نیازهای امنیت اطلاعات در روابط با تأمین‌کننده هستند و شایستگی‌های آن‌ها در سطح مورد انتظار به‌صورت منظم نگهداری می‌شود.	

۶-۲-۴-۲ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۴-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- در نظر گرفتن موارد زیر در برنامه‌های آموزش و آگاهی‌بخشی امنیت اطلاعات به‌عنوان قسمتی از فرایند مدیریت منابع انسانی: ۱- راهنماها و قوانین امنیت اطلاعات، مانند خط‌مشی امنیت اطلاعات و طبقه‌بندی اطلاعات، به خصوص برای کارکنان مرتبط با روابط با تأمین‌کننده؛	

۲- الزامات امنیت اطلاعاتی که به‌صورت عمومی در توافقنامه رابطه با تأمین‌کننده تعریف شده است، به‌منظور نمایش وجود چنین الزاماتی که نیازها و انتظارات کارفرما را برآورده می‌کند؛ ۳- عملکرد گذشته تأمین‌کننده با توجه به سطح انطباق با الزامات امنیت اطلاعات کارفرما، به‌منظور نمایش عدم پیروی بالقوه.	
ب- شناسایی و ارزیابی کارکنان با توجه به دسترسی و قابلیت آن‌ها برای افشا یا تغییر اطلاعات در رابطه با تأمین‌کننده، مانند اطلاعات حساس یا دارایی فکری که نباید افشا یا تغییر داده شود؛ پ- حصول اطمینان از این که کارکنان شناسایی‌شده، به خصوص آن‌هایی که در زمینه امنیت اطلاعات یا تصمیم‌گیری برای تدارک یا تأمین محصول یا خدمت دارای متعهد هستند، دارای صلاحیت و شایستگی‌های لازم هستند؛ ت- آموزش این کارکنان در مورد جنبه‌های امنیت اطلاعات روابط با تأمین‌کننده به خصوص برای حصول اطمینان از این که ساماندهی اطلاعات حساس به‌درستی درک شده است؛ ث- حصول اطمینان از این که بررسی‌های تفصیلی جنایی و پیشینه برای کارکنانی که دارای سمت‌های کلیدی در روابط با تأمین‌کننده هستند در مواردی که از لحاظ قانونی بلامانع است، انجام شده است. ج- تعیین نقاط تماس[1] و پشتیبان‌های[2] آن‌ها برای جنبه‌های بحرانی روابط با تأمین‌کننده شامل عملیات و نگهداری برای حصول اطمینان از تأثیر کمینه در زمانی که کارکنان سازمان را ترک می‌کنند.	

۶-۲-۵ فرایند مدیریت کیفیت

کارفرما	تأمین‌کننده
الف- کارفرما و تأمین‌کننده باید فرایند مدیریت کیفیتی را در زمان مدیریت امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند. **یادآوری**- هدف این فرایند حصول اطمینان از این موضوع است که محصولات و خدمات اهداف کیفی سازمان و رضایت مشتری را برآورده می‌کنند. الزامات یا توصیه‌های خاصی در زمانی که کارفرما و تأمین‌کننده به‌صورت داخلی این فرایند را	

1 - Contact Points
2 - Backups

پیاده‌سازی می‌کنند وجود ندارد.

۶-۳ فرایندهای پروژه

به فرایندهای پروژه مربوط‌به مدیریت و پشتیبانی سخت‌گیرانه پروژه با پوشش یک یا چند تـأمین‌کننـده است.

به خصوص، فرایندهای پروژه زیر ایجاد محیطی برای انجام یا طرح‌ریزی رابطه با تأمین‌کننده را پشتیبانی می‌کند:

الف- فرایند طرح‌ریزی پروژه؛

ب- فرایند ارزیابی و کنترل پروژه؛

پ- فرایند مدیریت تصمیم؛

ت- فرایند مدیریت مخاطرات؛

ث- فرایند مدیریت پیکربندی؛

ج- فرایند مدیریت اطلاعات؛

۶-۳-۱ فرایند طرح‌ریزی پروژه

۶-۳-۱-۱هدف

هدف زیر باید به‌منظور مدیریت موفق امنیـت اطلاعـات در فراینـد طـرح‌ریـزی پـروژه توسـط هریـک از سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- ایجاد فرایند طرح‌ریزی پروژه با پرداختن به امنیت اطلاعات روابط با تأمین‌کننده.	

۶-۳-۱-۲ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شـده در ۶-۲-۲-۱بند ۶-۳-۱-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- گنجاندن موارد زیر به‌عنوان قسمتی از فرایند طرح‌ریزی پروژه:	

۱) تأثیراتی بر روی هزینه پروژه، طرح‌ها و برنامه زمان‌بندی الزامات امنیت اطلاعاتی که برای دارایی‌های استفاده‌شده در تدارک یا تأمین محصول یا خدمت تعریف شده‌اند؛
۲) یکپارچه‌سازی امنیت اطلاعات با نقش‌ها، مسئولیت‌ها، پاسخگویی و اختیارات مرتبط پروژه؛
۳) ایمن‌سازی اطلاعات داخلی حساس، مانند اطلاعات مالی، مالکیت فکری و اطلاعات مربوط به مشتری یا کارکنان که می‌تواند توسط روابط با تأمین‌کننده تحت تأثیر قرار گیرد؛ و
۴) منابعی مانند منابع مالی که برای حصول اطمینان از محافظت از دارایی‌ها لازم هستند.

۶-۳-۲ فرایند کنترل و ارزیابی پروژه

کارفرما	تأمین‌کننده
الف- کارفرما و تأمین‌کننده باید فرایند کنترل و ارزیابی پروژه را در زمان مدیریت امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند. **یادآوری**- هدف این فرایند تعیین وضعیت پروژه و اجرای مستقیم طرح پروژه به‌منظور حصول اطمینان از اجرای پروژه بر طبق طرح‌ها و برنامه‌های زمان‌بندی در چارچوب بودجه پروژه به‌منظور برآورده کردن اهداف فنی است. الزامات یا توصیه‌های خاصی در زمانی که کارفرما و تأمین‌کننده به‌صورت داخلی این فرایند را پیاده‌سازی می‌کنند وجود ندارد. (برگرفته از ISO/IEC 15288)	

۶-۳-۳ فرایند مدیریت تصمیم

کارفرما	تأمین‌کننده
الف- کارفرما و تأمین‌کننده باید مدیریت تصمیم را در زمان مدیریت امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند. **یادآوری**- هدف این فرایند انتخاب مفیدترین اقدامات پروژه در شرایطی است که چند گزینه وجود دارد. الزامات یا توصیه‌های خاصی در زمانی که کارفرما و تأمین‌کننده به‌صورت داخلی این فرایند را پیاده‌سازی می‌کنند وجود ندارد. (برگرفته از ISO/IEC 15288)	

۶-۳-۴ فرایند مدیریت مخاطرات

۶-۳-۴-۱ هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند مدیریت مخاطرات توسط هریک از سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- پرداختن مداوم به مخاطرات امنیت اطلاعات در روابط با تأمین‌کننده و در چرخه حیات آن‌ها شامل بررسی مجدد آن‌ها به‌صورت دوره‌ای یا در زمان وقوع تغییرات کسب‌وکار، قانونی، مقرراتی، معماری، خط‌مشی‌ها و قراردادی	

۶-۳-۴-۲ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۲-۱بند ۶-۳-۴-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- تعریف، پیاده‌سازی، نگهداری، و بهبود چارچوب مدیریت امنیت اطلاعاتی که تحمل‌پذیری مخاطرات سازمانی را تعریف کند و قادر باشد برای شناسایی، ارزیابی، و تدبیر مخاطرات امنیت اطلاعات استفاده شود. این چارچوب همراه با موارد زیر است: ۱- نمونه‌های موجود تدارک یا تأمین محصول یا خدمت؛ ۲- تأمین‌کنندگان یا کارفرمایان درگیر در این نمونه‌ها؛ ۳- تدارک یا تأمین محصول یا خدمت. **یادآوری- استانداردهای ISO/IEC 27005 [۴]، ISO 31000 [۹] و ISO/IEC 15288 راهنمایی برای مدیریت مخاطرات فراهم می‌کنند.** **مراقبت‌های لازم باید برای حصول اطمینان از انطباق تعریف این چارچوب با موارد زیر انجام شود:** **۱-پیروی از کسب‌وکار یا مأموریت سازمان و در نظر گرفتن الزامات قانونی، مقرراتی، معماری، خط‌مشی‌ها و قراردادی قابل به‌کارگیری در سازمان.**	
۲- در نظر گرفتن ارزیابی تأمین‌کننده از نظر موارد زیر: i) تاریخچه گذشته، مانند ترتیبات[1] پیشین و کنونی کسب‌وکار و اطلاعات مربوط به اختلاف آن‌ها؛	۲-در نظر گرفتن ارزیابی کارفرما از نظر موارد زیر: i) تاریخچه گذشته، مانند سوابق پیشین و کنونی کسب‌وکار و اطلاعات مربوط به اختلاف آن‌ها؛ ii) توافق‌های قراردادی، مانند توافق‌های روابط با

1- Arrengements

ii) توافق‌های قراردادی، مانند توافق‌های روابط با تأمین‌کننده و توافق‌های عدم افشا؛ iii) پیامدهای امنیت اطلاعاتی تدارک محصول یا خدمت، شامل دارایی‌های ساماندهی‌شده، زیرساخت‌های فناوری مرتبط، وابستگی کسب‌وکار و پیمانکاران کسب‌وکار؛ iv) قابلیت تأمین‌کننده در نمایش بلوغ خود در زمینه امنیت اطلاعات. ۳- در نظر گرفتن موارد زیر در زمان تعریف روشی برای ارزیابی تأمین‌کننده: i) نوع ارزیابی برای به‌کارگیری در مورد تأمین‌کنندگان مانند خودارزیابی یا ارزیابی مستقل که توسط طرف سوم انجام شود؛ ii) سطح جزئیات ارزیابی و تواتر اجرای آن.	تأمین‌کننده و توافق‌های عدم افشا؛ iii) پیامدهای امنیت اطلاعاتی تأمین محصول یا خدمت، شامل موارد زیر: ۱- الزامات امنیت اطلاعات ارائه‌شده در اسناد مناقصه و توافقنامه رابطه با تأمین‌کننده؛ ۲- مخاطرات امنیت اطلاعات تأمین‌کننده که در نتیجه دسترسی کارفرما به اطلاعات تأمین‌کننده پدیدار می‌شود. نمونه‌ای از این مخاطرات در زمانی است که کارفرما سطحی از کنترل را بر فرایند ساخت تأمین‌کننده با دسترسی به اطلاعات حساس تأمین‌کننده انجام می‌دهد.
ب- به‌کارگیری این چارچوب مدیریت مخاطرات امنیت اطلاعات: ۱- طبقه‌بندی نمونه‌های موجود تدارک یا تأمین محصول یا خدمت؛ ۲- طبقه‌بندی تأمین‌کننده یا کارفرمای درگیر در این نمونه‌ها؛ ۳- در زمان: i) تعریف راهبرد رابطه با تأمین‌کننده یا کارفرما ii) طرح‌ریزی برای تدارک یا تأمین محصول یا خدمت. **یادآوری**- درصورتی‌که سازمان دارای گواهینامه ISO/IEC 27001 [۵] باشد، توصیه می‌شود دارایی‌های حاصل از تدارک یا تأمین محصول یا خدمت به‌منظور حصول اطمینان از ارزیابی و رفع مخاطرات امنیت اطلاعات در موجودی ISMS ذخیره شود.	

۶-۳-۵ فرایند مدیریت پیکربندی

کارفرما	تأمین‌کننده

الف- درصورتی‌که قابل‌کاربرد باشد، کارفرما و تأمین‌کننده باید فرایند مدیریت پیکربندی را در زمان اجرای امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند.

یادآوری ۱- هدف از این فرایند ایجاد و نگهداری یکپارچگی تمام خروجی‌های شناسایی‌شده پروژه یا فرایند و ایجاد امکان دسترسی به آن‌ها برای اشخاص علاقه‌مند است. الزامات یا توصیه‌های خاصی در زمانی که کارفرما و تأمین‌کننده به‌صورت داخلی این فرایند را پیاده‌سازی می‌کنند وجود ندارد. (برگرفته از ISO/IEC 15288)

یادآوری ۲- توصیه می‌شود، در زمان پیاده‌سازی فرایند مدیریت پیکربندی، ISO/IEC 27002 که راهنماهایی در مورد مدیریت تغییرات و روال‌های کنترل تغییرات فراهم می‌کند نیز در نظر گرفته شود.

۶-۳-۶ فرایند مدیریت اطلاعات

کارفرما	تأمین‌کننده
الف- کارفرما و تأمین‌کننده باید فرایند مدیریت اطلاعات را با در نظر گرفتن حساسیت اطلاعاتی که می‌تواند در مدت روابط با تأمین‌کننده تبادل شود، ایجاد کنند. **یادآوری ۱-** هدف از این فرایند فراهم کردن اطلاعات مرتبط، به‌موقع، کامل، معتبر، و در صورت لزوم، محرمانه برای اشخاص تعیین‌شده است. الزامات یا توصیه‌های خاصی در زمانی که کارفرما و تأمین‌کننده به‌صورت داخلی این فرایند را پیاده‌سازی می‌کنند وجود ندارد. (برگرفته از ISO/IEC 15288) **یادآوری ۲- ایجاد** ISMS **بر مبنای** ISO/IEC 27002 می‌تواند به‌عنوان مبنایی برای اعمال امنیت اطلاعات کافی در زمینه تبادل اطلاعات، به خصوص در مورد تغییرات امنیت اطلاعات و رخدادهای اتفاق‌افتاده در مدت روابط با تأمین‌کننده عمل کند.	

۶-۳-۷ فرایند سنجش

۶-۳-۷-۱ هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند سنجش توسط هریک از سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- جمع‌آوری، تحلیل، و گزارش سنجه‌های امنیت اطلاعات مرتبط با تدارک یا تأمین محصول یا خدمت به‌منظور نمایش بلوغ امنیت اطلاعات در روابط با تأمین‌کننده و به‌منظور پشتیبانی از مدیریت اثربخش فرایندها.	

۶-۳-۷-۲ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۲-۱بند ۶-۳-۷-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- تعریف، پیاده‌سازی نگهداری، و بهبود چارچوب سنجش امنیت اطلاعاتی که بتواند برای ارزیابی تدارک یا تأمین محصول یا خدمت استفاده شود. **یادآوری**- ISO/IEC 27004 [۱۰] راهنمایی‌هایی در مورد سنجش امنیت اطلاعات فراهم می‌کند که می‌تواند برای توسعه و پیاده‌سازی سنجه‌های مشخص مربوط به امنیت اطلاعات روابط با تأمین‌کننده به کار رود. مراقبت‌های لازم برای حصول اطمینان از این که این چارچوب مطابق با کسب‌وکار یا مأموریت سازمان و با در نظر گرفتن الزامات قانونی، مقرراتی، معماری، خط‌مشی‌ها و قراردادی قابل به‌کارگیری در سازمان تعریف شده است، باید به کار گرفته شود. ب- به‌کارگیری این چارچوب سنجش امنیت اطلاعات در زمان آماده‌سازی یک نمونه رابطه با تأمین‌کننده برای موافقت با شخص دیگری در مورد این که چه چیزی باید مورد سنجش قرار گیرد، چگونه سنجه‌ها گزارش شوند، تواتر گزارشگری و اقداماتی که باید در صورت عدم برآورده کردن معیارهای مشخص توسط سنجه‌ها انجام شود.	

۶-۴ فرایندهای فنی

فرایندهای فنی به‌صورت عمومی توسط تأمین‌کننده برای مقاصد زیر استفاده می‌شود:

الف- تعریف الزامات محصول یا خدمت؛

ب- تبدیل این الزامات به محصول یا خدمت اثربخش؛

پ- حفظ فراهم‌سازی خدمت یا محصول تدارک‌شده یا تأمین‌شده؛

ت- صدور اجازه بازتولید سازگار و باکیفیت محصول یا خدمت تدارک‌شده یا تأمین‌شده در مواقع ضروری؛ و

ث- امحای محصول یا خدمت، زمانی که تصمیم به بازنشستگی آن گرفته شده باشد.

یادآوری- ISO/IEC 27004 راهنمایی‌هایی در مورد سنجش امنیت اطلاعات فراهم می‌کند که می‌تواند برای توسعه و پیاده‌سازی سنجه‌های مشخص مربوط به امنیت اطلاعات روابط با تأمین‌کننده به کار رود.

۶-۴-۱ فرایند طراحی معمارانه

۶-۴-۱-۱ هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند طراحی معمارانه توسط هریک از سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده

الف- ایجاد چارچوب فنی برای تدارک مداوم محصول یا خدمت که هدف روابط با تأمین‌کننده را برآورده کند.

۶-۴-۱-۲فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۲-۱بند ۶-۴-۱-۶۱-۳-۱-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- ایجاد فرایندی برای تعریف، پیاده‌سازی، نگهداری و بهبود الزامات محصول یا خدمتی که می‌تواند تدارک یا تأمین شود، به‌منظور تسهیل انتخاب و مهاجرت آن.	

۷ امنیت اطلاعات در یک نمونه از رابطه با تأمین‌کننده

۷-۱ فرایند طرح‌ریزی رابطه با تأمین‌کننده

۷-۱-۱ هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند طرح‌ریزی رابطه با تأمین‌کننده توسط کارفرما محقق شود:

کارفرما
الف- ایجاد طرح رابطه با تأمین‌کننده که تصمیمات پذیرفته‌شده توسط مدیریت به‌منظور آغاز تدارک محصول یا خدمت و همچنین ملاحظات امنیت اطلاعات مربوط به طرح بالا را مستندسازی کند.

۷-۱-۲ ورودی‌ها

ورودی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند طرح‌ریزی رابطه با تأمین‌کننده توسط کارفرما در نظر گرفته شود:

کارفرما
الف- راهبرد رابطه با تأمین‌کننده؛ ب- انگیزه‌ها، نیازها و انتظارات مدیریت از تدارک محصول یا خدمت؛ ج- محدوده موردنظر محصول یا خدمتی که برای تدارک آن طرح‌ریزی شده است.

در صورت امکان؛

د) مستندات موجود مربوط به مدیریت رابطه با تأمین‌کننده، مانند طرح‌ها و توافقنامه‌های رابطه با تأمین‌کننده.

۷-۱-۳ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۲-۱بند ۷-۱-۱ اجرا شود:

کارفرما

الف- شناسایی و ارزیابی مخاطرات امنیت اطلاعاتی که اکتساب بالقوه محصول یا خدمت را همراهی می‌کنند، بر مبنای چارچوب مدیریت مخاطرات امنیت اطلاعاتی که در راهبرد رابطه با تأمین‌کننده تعریف شده است؛

کارفرما باید از ارزیابی مخاطرات امنیت اطلاعات زیر اطمینان حاصل کند:

۱) متناسب با امنیت محصول یا خدمتی باشد که برای تدارک آن طرح‌ریزی شده است؛

۲) محدودیت‌های قانونی و مقرراتی که بر محصول یا خدمت طرح‌ریزی‌شده برای ایجاد آن تأثیرگذار هستند، به‌منظور حصول اطمینان از این که مجوزها و گواهینامه‌های رسمی لازم، پیش از ورود به رابطه با تأمین‌کننده کسب شده باشد.

مراقبت‌های لازم در زمینه در نظر گرفتن تأثیرات بالقوه محصول یا خدمت موردنظر با توجه به مخاطرات امنیت اطلاعات مربوط به روابط موجود تأمین‌کننده باید در نظر گرفته شود. به خصوص درصورتی‌که وابستگی زیادی به تأمین‌کنندگان وجود داشته باشد.

ب- شناسایی سطح قابل‌پذیرش از مخاطرات مربوط به روابط بالقوه تأمین‌کننده.

پ- شناسایی و ارزیابی گزینه‌های تدبیر مخاطرات شناسایی‌شده و ارزیابی‌شده؛

ت- تعریف و پیاده‌سازی طرح تدبیر مخاطرات امنیت اطلاعات برای مخاطرات شناسایی‌شده و ارزیابی‌شده به‌منظور کاهش آن‌ها تا سطح قابل پذیرش مخاطرات

ج- ارائه توصیه‌های طرح ارزیابی و تدبیر مخاطرات امنیت اطلاعات به‌عنوان ورودی مذاکرات توافق رابطه با تأمین‌کننده؛

یادآوری- این اکتساب نباید درصورتی‌که امکان کاهش مخاطرات شناسایی‌شده امنیت اطلاعات تا سطح قابل‌قبول وجود ندارد، انجام شود.

چ) تعریف طرح رابطه با تأمین‌کننده برای محصول یا خدمتی که برای تدارک آن طرح‌ریزی‌شده و از

راهبرد رابطه با تأمین‌کننده پیروی می‌کند.

به خصوص، رابطه با تأمین‌کننده باید موارد زیر را در برگیرد:

۱) مشخصات محصول یا خدمت طرح‌ریزی‌شده برای تدارک، به خصوص محدوده، مخاطب، نوع و ماهیت آن؛

۲) دارایی‌ها، مانند کارسازها[1]، پایگاه داده‌ها[2]، زیرساخت شبکه، که به امنیت اطلاعات در استفاده از محصول یا خدمت مرتبط هستند، و مالکان مربوط به آن‌ها؛

۳) ورودی‌های طبقه‌بندی اطلاعات کارفرما به طبقه‌بندی اطلاعات تأمین‌کننده و دیگر کنترل‌های امنیت اطلاعات؛

۴) الزامات قانونی و مقرراتی قوانین حوزه قضایی کارفرما و محدوده قوانین و مقرراتی که تأمین‌کننده بالقوه مورد نظر را مقید نموده و باید در زمان انتخاب تأمین‌کننده بازنگری شود، مانند:

i) کنترل صادرات؛

ii) مقررات محافظت داده کارکنان و قوانین کار؛

iii) مالکیت فکری طرف‌های سوم؛ و

iv) الزامات قانونی و مقرراتی دیگر، مانند قوانین مالیاتی، مسئولیت محصول، قدرت‌های بررسی[3]

اگر هر مجوز یا گواهینامه‌ای از مراجع داخلی یا خارجی برای انطباق قانونی و مقرراتی لازم باشد، این موارد باید پیش از ورود به هر توافقی با تأمین‌کننده، کسب شود.

۵) نقش‌ها و مسئولیت‌های امنیت اطلاعات درون سازمان کارفرما که مخصوص محصول یا خدمتی هستند که ممکن است تدارک شود.

۶) اطلاعات کارفرما که می‌تواند با تأمین‌کنندگان بالقوه مورد نظر برای محصول یا خدمتی که ممکن است تدارک شود، به اشتراک گذاشته شود؛

یادآوری- اطلاعات کارفرما باید یک مالک معین داشته باشد که مسئول انتشار و حصول اطمینان از به‌کارگیری صحیح قوانین ساماندهی مربوط به آن باشد.

1 - Servers
2 - Databases
3 - Investigatory Powers

۷) الزامات کمینه امنیت اطلاعات که باید با تأمین‌کننده انتخاب‌شده برای تدارک محصول یا خدمت توافق شود.

این الزامات، باید به‌صورت مستقیم از طرح ارزیابی و تدبیر مخاطرات امنیت اطلاعات استخراج شود و چارچوب مخاطرات امنیت اطلاعات تعریف‌شده در راهبرد رابطه با تأمین‌کننده را تشکیل دهد.

همچنین، این الزامات باید با توجه به اهمیت محصول یا خدمتی که ممکن است تدارک و موارد زیر تعریف شود:

i) طبقه‌بندی اطلاعات انجام‌شده توسط کارفرما؛

ii) الزامات امنیت اطلاعات تعریف‌شده در طرح‌ها و توافقنامه‌های موجود رابطه با تأمین‌کننده.

تمامی الزامات تعریف‌شده باید به‌منظور تمایز با توصیه‌ها با واژه «باید» طبقه‌بندی شود.

۷-۱-۴ خروجی‌ها

خروجی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند طرح‌ریزی رابطه با تأمین‌کننده توسط کارفرما تولید شود:

کارفرما
الف- طرح ارزیابی و تدبیر مخاطرات امنیت اطلاعات مربوط به محصول یا خدمتی که ممکن است تدارک شود؛
ب- تصمیم مکتوب مدیریت مبنی بر تأیید طرح ارزیابی و تدبیر مخاطرات امنیت اطلاعات و امکان آغاز تدارک محصول یا خدمت؛
تصمیم عدم تدارک محصول یا خدمت نیز به همراه دلایل امنیت اطلاعاتی که موجب این تصمیم شده است باید مستندسازی شود.
ج- طرح رابطه با تأمین‌کننده.

۷-۲ فرایند انتخاب تأمین‌کننده

۷-۲-۱ اهداف

اهداف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند انتخاب تأمین‌کننده توسط هریک از سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- انتخاب تأمین‌کننده‌ای که امنیت اطلاعات کافی را برای محصول یا خدمتی که ممکن است تدارک شود، فراهم کند.	الف- پاسخ به اسناد مناقصه کارفرما با در نظر گرفتن مخاطرات امنیت اطلاعات مربوط به محصول یا خدمتی که قصد تأمین آن وجود دارد و الزامات امنیت اطلاعات اسناد مناقصه کارفرما (مانند ITT، RFP)

۷-۲-۲ ورودی‌ها

ورودی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند انتخاب تأمین‌کننده توسط هر یک از سازمان‌های زیر در نظر گرفته شود:

کارفرما	تأمین‌کننده
الف- راهبرد رابطه با تأمین‌کننده؛ ب- طرح رابطه با تأمین‌کننده. در صورت کاربست‌پذیری: پ- معیارهای موجود انتخاب تأمین‌کننده تعریف‌شده برای دیگر محصولات یا خدمات تدارک‌شده؛ ت- توافقنامه‌های محرمانگی موارد تعریف‌شده برای دیگر محصولات یا خدمات تدارک‌شده.	الف- راهبرد رابطه کارفرما؛ ب- توافقنامه محرمانگی کارفرما؛ ج- اسناد مناقصه کارفرما.

۷-۲-۳ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۲-۱بند ۷-۲-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- تعریف و پیاده‌سازی معیارهای انتخاب تأمین‌کننده مبتنی بر طرح رابطه با تأمین‌کننده‌ای که شامل مشخصه‌های محصول یا	الف- بازنگری توافقنامه محرمانگی به‌منظور حصول اطمینان از این که این توافقنامه از دارایی‌های تأمین‌کننده مانند اطلاعات و

خدمتی که ممکن است تدارک شود و چارچوب معیارهای انتخاب تأمین‌کننده‌ای که در راهبرد رابطه با تأمین‌کننده تعریف شده است؛

معیارهای انتخاب تأمین‌کننده باید موارد زیر را پوشش دهد؛

۱- پذیرش از سوی تأمین‌کننده الزامات امنیت اطلاعات تعریف شده در اسناد مناقصه؛

۲- بلوغ تأمین‌کننده در زمینه امنیت اطلاعات؛

این بلوغ می‌تواند با درخواست از تأمین‌کننده برای دارا بودن گواهینامه ISO/IEC 27001 یا فراهم کردن مستندات امنیت اطلاعات مانند طرح‌های تداوم کسب‌وکار مستندشده و آزمون‌شده برای حصول اطمینان از ظرفیت پشتیبانی از فعال‌سازی‌های همزمان توسط کارفرمایان طرح‌های مدیریت و بازیابی رخدادها، تعریف شود.

۳- شرایطی که در آن تأمین‌کننده اجازه ممیزی توسط کارفرما یا طرف سوم مجاز را به‌منظور اثبات انطباق با الزامات امنیت اطلاعات تعریف‌شده فراهم می‌کند؛

۴- پذیرش انتقال در زمانی که محصول یا خدمتی که ممکن است تدارک شود پیش از این توسط کارفرما یا تأمین‌کننده دیگری بهره‌برداری یا ساخته شده باشد؛

۵-پذیرش خاتمه برای نگهداری امنیت اطلاعات در مورد خاتمه توافق تأمین‌کننده؛

۶- مدیریت ظرفیت تأمین‌کننده برای تأمین محصول یا خدمتی که ممکن است تدارک شود،

۷- قدرت مالی تأمین‌کننده‌ای که ممکن است محصول یا خدمت را تأمین کند؛ و

سامانه‌های اطلاعاتی منتقل‌شده در طول فرایند انتخاب تأمین‌کننده محافظت می‌کند؛

یادآوری۱- در غیاب توافقنامه محرمانگی که توسط کارفرما پیشنهادشده باشد، توصیه‌می‌شود، تأمین‌کننده توافقنامه محرمانگی خود را پیش از هرگونه تبادل دارایی که می‌تواند بر محصول یا خدمت تأمین‌شده تأثیرگذار باشد، به کارفرما ارائه دهد.

یادآوری۱- بهتر است توافقنامه‌های محرمانگی موجود به عنوان پشتیبانی برای آماده‌سازی توافقنامه محرمانگی محصول یا خدمتی که ممکن است تأمین شود، مورد استفاده قرار گیرد.

ب- حصول توافق و امضای توافقنامه محرمانگی کارفرما؛

پ- دریافت سند مناقصه کارفرما؛

ت- اعتبارسنجی این که توسعه و تأمین محصول یا خدمت از استانداردهای کسب‌وکاری و فنی پذیرفته‌شده رایج و تجارب برتر پیروی می‌کند؛

ث- شناسایی و ارزیابی مخاطرات امنیت اطلاعاتی که تأمین بالقوه محصول یا خدمت را همراهی می‌کند، بر مبنای چارچوب مدیریت مخاطرات امنیت اطلاعات تعریف‌شده در راهبرد رابطه کارفرما؛

توصیه می‌شود، مراقبت‌های لازم توسط تأمین‌کننده باید برای حصول اطمینان از این که تأمین محصول یا خدمت مخاطرات امنیت اطلاعات مربوط به فعالیت‌ها و روابط جاری کسب‌وکار را افزایش نمی‌دهد، در نظر گرفته شود.

ج- شناسایی سطح قابل پذیرش مخاطرات برای تأمین محصول یا خدمت؛

۸- محل تأمین‌کننده و محلی که از آن محصول یا خدمت تأمین خواهد شد.

مراقبت‌های ویژه‌ای در مورد این محل باید در رابطه با موارد زیر صورت گیرد:

i) شناسایی مخاطرات بالقوه قانونی و مقرراتی ایجادشده در اثر تفاوت‌های قانون و مقررات کارفرما و تأمین‌کننده؛

یادآوری- نیاز است بررسی‌های مربوط به قوانین خارجی در زمان اکتساب بین‌حوزه‌ای[1] انجام شود.

ii) حصول اطمینان از این که تعهدات قانونی و مقرراتی که برای تأمین‌کننده وجود دارد، نمی‌تواند اثرات منفی از نظر امنیت اطلاعات بر روی رابطه با تأمین‌کننده داشته باشد.

iii) ارزیابی تهدیدهای محیطی مانند نرخ جرائم محلی یا مسائل جغرافیایی و تأثیرات بالقوه آن‌ها.

یادآوری- معیارهای موجود انتخاب تأمین‌کننده که برای محصول یا خدمت تدارک‌شده دیگری تعریف شده است نیز می‌تواند در زمان تعریف و پیاده‌سازی معیارهای انتخاب تأمین‌کننده محصول یا خدمتی که ممکن است تدارک شود نیز استفاده شود.

ب- آماده‌سازی توافقنامه محرمانگی برای امضا توسط تأمین‌کننده‌ی بالقوه برای محافظت از دارایی‌های کارفرما، مانند اطلاعات و سامانه‌های اطلاعاتی که در طول فرایند انتخاب تأمین‌کننده منتقل می‌شود؛

یادآوری ۱ - درصورتی‌که مناسب باشد، بهتر است این توافقنامه محرمانگی قبل از هرگونه تبادل اطلاعات مربوط به محصول یا خدمتی که ممکن است تدارک شود، توسط

چ) شناسایی و ارزیابی گزینه‌های تدبیر مخاطرات شناسایی‌شده و ارزیابی‌شده؛

ح- تعریف و پیاده‌سازی طرح تدبیر مخاطرات امنیت اطلاعات برای مخاطرات شناسایی‌شده و ارزیابی‌شده که برای کاهش آن‌ها تا سطح قابل پذیرش مخاطرات انتخاب شده‌اند؛

یادآوری- این تأمین نباید در صورتی که امکان کاهش مخاطرات شناسایی‌شده امنیت اطلاعات تا سطح قابل قبول وجود ندارد، انجام شود.

خ- بازنگری الزامات امنیت اطلاعات تعریف‌شده در سند مناقصه به‌منظور:

۱- حصول اطمینان از انطباق با این الزامات؛

۲- تعیین این که آیا نیاز به پیاده‌سازی کنترل‌های امنیت اطلاعات دیگری در راستای پرداختن به این الزامات وجود دارد.

منابع لازم، مانند منابع مالی، برای پیاده‌سازی این کنترل‌ها باید برای حصول اطمینان از این که تأمین‌کننده تمایل به پاسخگویی به سند مناقصه را دارد، ارزیابی شود.

د- بازنگری شرایطی که در آن ممیزی توسط کارفرما یا طرف سوم مجاز به‌منظور اثبات انطباق با الزامات امنیت اطلاعات تعریف‌شده توسط کارفرما انجام خواهد شد.

ذ- تصمیم‌گیری برای پاسخگویی یا عدم پاسخگویی به سند مناقصه بر مبنای موارد زیر:

۱- طرح ارزیابی و تدبیر مخاطرات امنیت اطلاعات تأمین‌کننده مربوط به تأمین بالقوه

1 - cross jurisdictional

کارفرما و تأمین‌کننده بالقوه امضا شود. **یادآوری۲** – بهتر است توافقنامه‌های محرمانگی موجود به‌عنوان پشتیبانی برای آماده‌سازی توافقنامه محرمانگی محصول یا خدمتی که ممکن است تدارک شود، مورد استفاده قرار گیرد. پ- آماده‌سازی و فراهم کردن سند مناقصه‌ای مانند ITT یا RFP برای تأمین‌کننده بالقوه؛ سند مناقصه باید بر مبنای طرح رابطه با تأمین‌کننده تولید شده و باید شامل اطلاعات کافی برای توانمندسازی تأمین‌کننده در راستای تدارک با منطق طرح پیشنهاد خود باشد. به خصوص سند مناقصه باید شامل موارد زیر باشد: ۱- مشخصات (مانند محدوده، مخاطب، نوع و ماهیت)محصول یا خدمتی که قرار است تدارک شود؛ ۲- الزامات امنیت اطلاعاتی که تأمین کننده باید در زمان تأمین محصول یا خدمت رعایت کند؛ ۳- شاخص‌های سطح خدمات[1] یا شاخص‌های کلیدی عملکرد برای پیگیری در زمان تأمین محصول یا خدمت؛ و ۴- جریمه‌های بالقوه‌ای که می‌تواند توسط کارفرما برای موارد عدم انطباق با الزامات امنیت اطلاعات در نظر گرفته شود. **یادآوری** – سند مناقصه بهتر است تا حد امکان تنها شامل اطلاعات عمومی و یا طبقه‌بندی‌نشده باشد. چنین	محصول یا خدمت؛ ۲- شکافی که برای برآورده‌کردن الزامات امنیت اطلاعات کارفرما در سند مناقصه مورد رسیدگی قرار گیرد. ر- انتصاب فردی با مسئولیت یکپارچه‌سازی زبان امنیت اطلاعات مناسب که به الزامات و معیارهای امنیت اطلاعات در سند پاسخ بپردازد.

1 - Service level

سندی بهتر است تنها شامل اطلاعات ضروی برای فراهم کردن امکان پاسخدهی منطقی از سوی تأمین‌کننده باشد. توصیه می‌شود، اطلاعات با حساسیت بالا هرگز تحت هیچ‌شرایطی در سند مناقصه گنجانده نشود. ت- جمع‌آوری اسناد پاسخی که توسط تأمین‌کنندگان بالقوه مورد نظر در پاسخ به سند مناقصه ارسال شده و ارزیابی آن ها بر مبنای معیارهای انتخاب تأمین‌کننده؛ و **یادآوری** – برای تدارک خدمات غیرقابل‌سفارشی‌سازی (مانند خدمات ASP)، توصیه‌می‌شود کارفرما برآورده‌شدن معیارهای انتخاب تأمین‌کننده در مدیریت، کنترل‌ها، پیاده‌سازی، و سطوح خدمات امنیت اطلاعات فراهم‌شده توسط تأمین‌کننده را اعتبارسنجی نماید. ث- انتخاب تأمین‌کننده بر مبنای ارزیابی این اسناد پاسخ. **یادآوری** – توصیه می‌شود، کارفرمایان تأمین‌کننده‌ای را ترجیح دهند که شفافیت بیشتری در زنجیره تأمین محصول یا خدمت دارد و در مورد برآورده‌کردن الزامات امنیت اطلاعات تعریف‌شده در سند مناقصه کارفرما اطمینان دهد.	

۷-۲-۴ خروجی‌ها

خروجی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند انتخاب تأمین‌کننده توسط هر یک از سازمان‌های زیر تولید شود:

کارفرما	تأمین‌کننده
الف- معیارهای انتخاب تأمین‌کننده؛ ب- توافقنامه محرمانگی؛ پ- سند مناقصه؛ ت- نتایج ارزیابی اسناد پاسخ؛ ث- انتخاب تأمین‌کننده‌ی بالقوه‌ای که معیارهای	الف- در صورت امکان، توافقنامه محرمانگی امضاشده کارفرما؛ ب- طرح ارزیابی و تدبیر مخاطرات امنیت اطلاعات مربوط به محصول یا خدمتی که ممکن است تأمین شود؛

انتخاب تأمین‌کننده را برآورده کرده است، توسط کارفرما.	پ- سند پاسخ به سند مناقصه کارفرما.

۷-۳ فرایند حصول توافق با تأمین‌کننده

۷-۳-۱ هدف

هدف زیر باید به‌منظور مدیریت مطلوب امنیت اطلاعات در فرایند حصول توافق با تأمین‌کننده توسط سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- ایجاد و توافق برسر توافقنامه رابطه با تأمین‌کننده که به موارد زیر بپردازد: ۱- نقش‌ها و مسئولیت‌های امنیت اطلاعات کارفرما و تأمین‌کننده؛ ۲- فرایند انتقال در مواقعی که محصول یا خدمت پیش از این توسط شخصی به‌غیر از تأمین‌کننده بهره‌برداری یا ساخته شده است؛ ۳- مدیریت تغییر امنیت اطلاعات؛ ۴- مدیریت رخدادهای امنیت اطلاعات؛ ۵-پایش و اعمال انطباق؛ ۶- فرایند خاتمه.	

۷-۳-۲ ورودی‌ها

ورودی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند حصول توافق با تأمین‌کننده توسط هر یک از سازمان‌های زیر در نظر گرفته شود:

کارفرما	تأمین‌کننده
الف- راهبرد رابطه با تأمین‌کننده؛	الف- راهبرد رابطه کارفرما؛
ب- اسناد مناقصه کارفرما؛ پ- سند پاسخ تأمین‌کننده.	

۷-۳-۳ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده کردن اهداف تعریف‌شده در ۶-۲-۲-۱بند ۷-۳-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- تعریف توافقنامه رابطه با تأمین‌کننده ویژه تأمین محصول یا خدمت طرح‌ریزی‌شده با طرف مقابل؛ این توافقنامه باید: ۱- با سند مناقصه کارفرما و سند پاسخ تأمین‌کننده انطباق داشته باشد؛ به این معنی که این توافقنامه به خصوص شامل موارد زیر باشد: i) الزامات امنیت اطلاعاتی که تأمین‌کننده باید مطابق آن‌ها رفتار کند؛ ii) شاخص‌های سطوح خدمت یا شاخص‌های کلیدی عملکرد برای پیروی در زمان ارائه محصول یا خدمت. **یادآوری** – در مورد خدمات بدون قابلیت سفارشی‌شدن (مانند خدمت ASP) محتوای توافقنامه تأمین‌کننده می‌تواند از سند مناقصه یا سند پاسخ استخراج شود. ۲- توجه به نقش‌ها و مسئولیت‌های امنیت اطلاعات هر دو طرف کارفرما و تأمین‌کننده در محدوده تأمین محصول یا خدمت؛ **یادآوری** – نقش‌ها و مسئولیت‌های تعریف‌شده باید به افراد شایسته‌ای در سازمان کارفرما یا تأمین‌کننده سپرده شود که به‌صورت صحیح و منظم در زمینه امنیت اطلاعات آموزش دیده باشند. ۳- توجه به جنبه‌های امنیت اطلاعات سوابق پیمانکاری فرعی تأمین‌کننده که بر تأمین محصول یا خدمت تأثیرگذار است؛ ۴- توجه به انتقال تأمین محصول یا خدمت به‌منظور حصول اطمینان از ادامه‌دار بودن آن، در مواقعی که محصول پیش‌ازاین توسط کارفرما یا تأمین‌کننده دیگری ساخته یا بهره‌برداری شده است؛ طرح انتقالی باید با مشخص کردن الزامات امنیت اطلاعاتی برای پیروی از سوی کارفرما و تأمین‌کننده در زمان انتقال محصول یا خدمت تعریف شود. تعریف این طرح باید با الزامات امنیت اطلاعات سطح بالای مرتبط که در راهبردهای رابطه کارفرما و تأمین‌کننده تعریف شده است، انطباق داشته باشد. طرح انتقال باید از سوی هر دو طرف کارفرما و تأمین‌کننده موردتوافق قرار گیرد و در توافقنامه رابطه با تأمین‌کننده مستندسازی شود.	

۵- توجه به ساماندهی تغییرات و رخدادها، رخنه‌ها و دیگر رویدادهایی که می‌تواند بر روی امنیت اطلاعات کارفرما و تأمین‌کننده تأثیرگذار باشد و در محدوده محصول یا خدمت موردنظر جا دارد؛

به خصوص:

i) روش‌اجرایی مدیریت تغییرات امنیت اطلاعات باید تعریف شود، توسط کارفرما و تأمین‌کننده موردتوافق قرار گیرد و در توافقنامه رابطه با تأمین‌کننده مستندسازی شود. این کار برای حصول اطمینان از تأیید فوری تغییرات توسط کارفرما و انجام آن‌ها توسط تأمین‌کننده ضروری است.

ii) روش اجرایی مدیریت رخدادهای امنیت اطلاعات باید تعریف شود، توسط کارفرما و تأمین‌کننده موردتوافق قرار گیرد و در توافقنامه رابطه با تأمین‌کننده مستندسازی شود. این کار برای حصول اطمینان از شناسایی، گزارش و رسیدگی فوری به رخدادهای اتفاق‌افتاده در زمان تأمین محصول یا خدمت با در نظر گرفتن ملاحظات و الزامات قانونی، مقرراتی و ساختاری ضروری است.

یادآوری – استاندارد ISO/IEC 27035 [۶] راهنمایی در مورد مدیریت رخدادهای امنیت اطلاعات فراهم می‌کند.

تعریف هر دو روش اجرایی باید با الزامات مرتبط سطح بالای امنیت اطلاعات در راهبرد رابطه کارفرما و تأمین‌کننده انطباق داشته باشد.

۶- بیان چگونگی موارد زیر:

۱- پایش و اعمال انطباق تأمین‌کننده با الزامات تعریف‌شده امنیت اطلاعات، توسط کارفرما؛ و

۲- تعهد تأمین‌کننده به الزامات انطباق[1]

به خصوص، عناصر زیر باید توسط هریک از سازمان‌های زیر پیاده‌سازی شود و در توافقنامه رابطه با تأمین‌کننده مستندسازی شود:

i) در سمت کارفرما:

۱- طرحی مخصوص پایش و اعمال انطباق که مطابق الزامات مرتبط سطح بالای امنیت اطلاعات در راهبرد رابطه با تأمین‌کننده باشد و موارد زیر را توضیح دهد:

الف- نوع فعالیت‌های پایش، مانند تحلیل و ممیزی مخاطرات امنیت اطلاعات، تواتر[2] اجرای آن‌ها و نحوه گزارش نتایج آن‌ها؛ و

ب- مدیریت و پیگیری اقدامات اصلاحی آغازشده از سوی تأمین‌کننده.

ii) در سمت تأمین‌کننده:

1 - compliance requirements.
2 - Frequency

۱- شناسایی، آغاز، مدیریت، ثبت، گزارش و بستن اقدامات اصلاحی حاصل از نتایج فعالیت‌های پایش و اعمال کارفرما.

این فرایند باید با الزامات مرتبط سطح بالای امنیت اطلاعات در راهبرد رابطه کارفرما انطباق داشته باشد.

۷- توجه به مالکیت دارایی فکری محصول یا خدمتی که ممکن است تأمین شود و دارایی‌های مرتبط با آن‌که توسط کارفرما و تأمین‌کننده ایجاد خواهد شد؛

۸- توجه به شرایطی که تحت آن‌ها کارفرما یا تأمین‌کننده حق خاتمه توافق در زمان اجرای آن‌ها را دارد، مانند عدم توانایی تأمین‌کننده در برآورده کردن الزامات امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده؛

۹- توجه به جریمه‌هایی که در صورت عدم انطباق با الزامات امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده از سوی کارفرما یا تأمین‌کننده تحمیل خواهد شد؛ و

۱۰- تعریف تعهدات امنیت اطلاعات و الزامات تداوم خدمات مربوط به اجرای خاتمه رابطه با تأمین‌کننده؛

طرح خاتمه باید تعریف شود، توسط کارفرما و تأمین‌کننده موردتوافق قرار گیرد و در توافقنامه رابطه با تأمین‌کننده مستندسازی شود.

تعریف طرح خاتمه باید الزامات مرتبط سطح بالای امنیت اطلاعات در راهبرد رابطه کارفرما و تأمین‌کننده انطباق داشته باشد.

به خصوص، طرح خاتمه باید موارد زیر را پوشش دهد:

i) تعریف الزامات امنیت اطلاعاتی که در صورت تصمیم به‌منظور بازگرداندن تأمین محصول یا خدمت از تأمین‌کننده به کارفرما یا تأمین‌کننده‌ای دیگر، باید از سوی کارفرما و تأمین‌کننده پیروی شود؛

ii) شناسایی دارایی‌هایی (مانند اطلاعات و سامانه‌های اطلاعاتی کارفرما، اطلاعات و سامانه‌های اطلاعاتی تأمین‌کننده، سوابق[1]) که در تأمین محصول یا خدمت استفاده شده‌اند. این کار برای انتخاب دارایی‌هایی با شرایط زیر انجام می‌شود:

۱- دارایی‌هایی که به کارفرما بازگشت داده یا به تأمین‌کننده دیگری فرستاده خواهد شد؛

۲- دارایی‌هایی که به تأمین‌کننده بازگشت داده خواهد شد؛

۳- دارایی‌هایی که امحا شده و یا توسط کارفرما یا تأمین‌کننده نگهداری خواهد شد؛

1 - Records

iii) سازوکارهای انتقال برای به‌کارگیری در مورد دارایی‌هایی که برای بازگشت به کارفرما یا فرستادن به تأمین‌کننده دیگر یا بازگشت به تأمین‌کننده شناسایی شده‌اند؛

iv) سازوکارهای امحا[1] برای به‌کارگیری در مورد دارایی‌هایی که برای امحا شناسایی شده‌اند؛

یادآوری – امحا می‌تواند در قاب‌های زمانی[2] که توسط کارفرما و تأمین‌کننده موردتوافق قرار می‌گیرد و یا توسط قانون یا مقررات تعیین می‌شود، الزام شود. امحا می‌تواند به‌وسیله سازوکارهای حفاظت از امنیتی که توسط کارفرما و تأمین‌کننده تعریف و توافق شده است و برای دارایی‌های نگهداری‌شده اعمال شود. یک توافقنامه عدم افشای ویژه نیز می‌تواند برای حصول اطمینان از حفاظت از دارایی‌های نگهداری‌شده بعد از خاتمه رابطه با تأمین‌کننده میان کارفرما و تأمین‌کننده تعریف و توافق شود.

v) قابلیت‌های حصول اطمینانی که انجام‌شدن امحای دارایی‌های انتخاب‌شده را نشان دهند.

توصیه می‌شود حصول اطمینان باید با یک گواهینامه امحا پشتیبانی شود.

یادآوری – کارفرما و تأمین‌کننده، هر دو می‌توانند صحت‌سنجی مستقلی را نیز در مورد امحای مناسب دارایی‌ها الزام نمایند.

vi)دوره تحویل[3] با آموزش مربوط به آن که در صورت اتخاذ تصمیمی مبنی بر بازگشت تأمین محصول یا خدمت به کارفرما یا انتقال آن به تأمین‌کننده دیگر، به‌کارگرفته خواهد شد؛

vii) تعهد به عدم افشای اطلاعات حساس در مدت‌زمانی بعد از خاتمه توافق با تأمین‌کننده؛

viii) مقیاس زمانی اجرای روش اجرایی خاتمه.

یادآوری – نیاز است چند حوزه کسب‌وکاری مختلف که نماینده فعالیت‌های تجاری، فنی و اکتساب هستند، به دلیل تأثیرات امنیت میان سازمان‌ها، در مذاکرات توافقنامهب رابطه با تأمین‌کننده درگیر باشند. این کار بهتر است اطمینان دهد که این توافقنامه علایق بیشینه تعداد واحدهای سازمانی ممکن که تحت تأثیر محصول یا خدمت تأمین‌شده قرار گرفته‌اند را در نظر می‌گیرد و در زمینه پرداختن به مخاطرات و دغدغه‌های امنیت اطلاعات جامع‌تر است.

ب- تأیید توافقنامه رابطه با تأمین‌کننده تعریف‌شده با طرف مقابل.

۷-۳-۴ خروجی‌ها

خروجی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند حصول توافق با تأمین‌کننده توسط هر یک از سازمان‌های زیر تولید شود:

1 - Destruction
2 - Time Frames
3 - Hand-over

کارفرما	تأمین‌کننده
الف- توافقنامه امضاشده رابطه با تأمین‌کننده؛ **یادآوری** – توصیه می‌شود، توافقنامه امضاشده رابطه با تأمین‌کننده به صورتی ذخیره شود که قابلیت ردیابی[1] و یکپارچگی آن در کنار دسترس‌پذیری و محرمانگی مورد محافظت قرار گیرد. ب- روش اجرایی مدیریت تغییرات امنیت اطلاعات؛ پ- روش اجرایی مدیریت رخدادهای امنیت اطلاعات؛ ت- طرح خاتمه. در صورت کاربست‌پذیری؛ ث- طرح انتقال. **یادآوری** – روش‌های رایج تبادل اطلاعات (مانند اتصال شبکه، پیام‌رسانی و قالب‌های پرونجا، نسخه‌های نرم‌افزار، استانداردهای رمزنگاشتی[2]) نیز بهتر است برای فعال‌سازی ارتباطات بین کارفرما و تأمین‌کننده با محرمانگی، یکپارچه‌سازی و دسترس‌پذیری کافی ایجاد شود.	
ج- طرح و روش‌های اجرایی پایش انطباق و اعمال آن توسط کارفرما.	چ- پذیرش طرح و روش‌های اجرایی پایش انطباق و اعمال آن. ح) فرایند ساماندهی اقدامات اصلاحی.

۷-۴ فرایند مدیریت رابطه با تأمین‌کننده

۷-۴-۱ اهداف

اهداف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند مدیریت رابطه با تأمین‌کننده توسط سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف- نگهداری امنیت اطلاعات در مدت‌زمان اجرای رابطه با تأمین‌کننده در انطباق با توافقنامه رابطه با تأمین‌کننده و به خصوص با در نظر گرفتن موارد زیر:	

1 - Traceability
2 - Cryptographic

۱- انتقال تأمین محصول یا خدمتی که پیش از این توسط کارفرما یا تأمین‌کننده دیگری بهره‌برداری یا ساخته شده باشد.	۱- پشتیبانی از کارفرما در انتقال تأمین محصول یا خدمتی که پیش‌ازاین توسط کارفرما یا تأمین‌کننده دیگری بهره‌برداری یا ساخته شده باشد.
۲- آموزش کارکنانی که تحت تأثیر الزامات امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده قرار گرفته‌اند؛ ۳- مدیریت تغییرات و رخدادهایی که می‌تواند بر روی تأمین محصول یا خدمت تأثیرگذار باشد؛	
۴- پایش و اعمال انطباق تأمین‌کننده با شرایط امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده.	۴- پشتیبانی از کارفرما در فعالیت‌های پایش و اعمال انطباق.

۷-۴-۲ ورودی‌ها

خروجی‌های بند ۷-۲-۷۴-۳-۴ باید توسط کارفرما و تأمین‌کننده به‌عنوان ورودی‌های کمینه در زمان اجرای فعالیت‌های امنیت اطلاعات مرتبط با فرایند مدیریت رابطه با تأمین‌کننده در نظر گرفته شود.

توصیه می‌شود، ورودی‌های زیر نیز توسط هر یک از سازمان‌های زیر در نظر گرفته شود:

کارفرما	تأمین‌کننده
الف- تصمیمات مربوط به کسانی‌که فعالیت‌های پایش و اعمال انطباق تأمین‌کننده را انجام می‌دهند؛ ب- نتایج پیشین فعالیت‌های پایش و اعمال انطباق تأمین‌کننده و روندها در طول زمان.	الف- نتایج پیشین فعالیت‌های پایش و اعمال انطباق تأمین‌کننده که توسط کارفرمایان محصولات یا خدمات تأمین‌شده، انجام شده است.

۷-۴-۳ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده‌کردن اهداف تعریف‌شده در ۶-۲-۲-۱بند ۷-۴-۱ اجرا شود:

کارفرما	تأمین‌کننده

الف- حصول اطمینان از این که طرف مقابل توافقنامه رابطه با تأمین‌کننده را دریافت کرده است و جنبه‌های امنیت اطلاعات موجود در آن را به‌صورت کامل درک کرده است.

ب- بهره‌برداری کردن انتقال محصول یا خدمت با توجه به طرح انتقال توافق‌شده و اعلام به طرف مقابل در صورت وقوع رویدادهای غیرمترقبه در مدت این فعالیت در اسرع وقت؛

پ- مدیریت تغییرات و رخدادهای امنیت اطلاعات با توجه به روش‌های اجرایی توافق‌شده؛

ت- آموزش منظم کارکنانی که می‌توانند در اجرای طرح خاتمه درگیر شوند؛

ث- مدیریت تغییرات دیگر، مانند موارد زیر، در زمانی که از سوی طرف مقابل اعلام شود، و توسط روش اجرایی مدیریت تغییر امنیت اطلاعات پوشش داده نشده باشد و قادر به تأثیرگذاری بر روی تأمین محصول یا خدمت تدارک‌شده باشد:

۱- تغییر در کسب‌وکار، مأموریت یا محیط سازمان؛

۲- تغییرات مرتبط به قدرت مالی سازمان؛

۳- تغییر مالکیت، یا ایجاد سرمایه‌های مشترک؛

۴- تغییر محلی که محصول یا خدمت از آنجا تدارک یا تأمین می‌شود؛

۵-تغییر سطح امنیت اطلاعات سازمان، مانند اکتساب یا ازدست‌دادن گواهینامه ISO/IEC 27001؛

۶- تغییر در توانایی پشتیبانی از قابلیت‌های تداوم کسب‌وکار؛ و

۷) تغییر در الزامات قانونی، مقرراتی و قراردادی کاربردی در مورد سازمان.

مدیریت این تغییرات نیازمند اجرای موارد زیر از سوی شخصی است که تغییرات به وی اطلاع‌رسانی شده است:

۱- حصول اطمینان از این که مخاطرات امنیت اطلاعات مربوط به این سطح از تغییرات در کنار سایر گزینه‌ها برای تدابیر مربوطه شناسایی و ارزیابی شده است؛

۲- حصول اطمینان از این که طرح تدبیر مخاطرات برای مخاطرات شناخته‌شده امنیت اطلاعات به‌منظور کاهش آن‌ها، شناسایی شده است و توسط اشخاص درگیر توافق شده و پیاده‌سازی شده است؛

یادآوری – توصیه می‌شود تدارک یا تأمین محصول یا خدمت در زمانی که امکان کاهش مخاطرات شناسایی‌شده تا سطح قابل پذیرش وجود ندارد، خاتمه یابد.

۳- توافق با طرف مقابل در مورد تغییرات توافقنامه رابطه با تأمین‌کننده، که شامل موارد زیر است:

i) روش اجرایی مدیریت تغییرات امنیت اطلاعات؛

ii) روش اجرایی مدیریت رخدادهای امنیت اطلاعات و

iii) طرح خاتمه.

۴- تأیید توافقنامه به‌روزرسانی‌شده رابطه با تأمین‌کننده.

ج- حصول اطمینان از این که فعالیت‌های پایش و اعمال انطباق، طرح مربوط به آن و فرایند ساماندهی اقدامات اصلاحی را برآورده کرده است.

در مورد تغییرات مخاطرات امنیت اطلاعات یا عدم تطابق‌های ممیزی، کارفرما باید با پشتیبانی تأمین‌کننده موارد زیر را انجام دهد:

۱- شناسایی و ارزیابی تأثیرات امنیت اطلاعات حاصل‌شده از این تغییرات و عدم تطابق‌ها؛

۲- تعیین این که آیا جنبه‌های امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده نیاز به بازنگری دارند یا خیر؛

۲- تعیین اقدامات اصلاحی که بهتر است در مقیاس زمانی تعریف‌شده و توافق‌شده برای دستیابی به سطح قابل‌پذیرش امنیت اطلاعات در محدوده محصول یا خدمت تدارک‌شده انجام شود؛

۴- توافق با تأمین‌کننده در مورد:

i) تغییراتی که بر روی جنبه‌های امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده انجام شود؛ و

ii) پیاده‌سازی اقدامات اصلاحی؛

۵-تأیید توافقنامه به‌روزرسانی‌شده رابطه با تأمین‌کننده.

ج- پشتیبانی از فعالیت‌های پایش و اعمال انطباق کارفرما با توجه به طرح و فرایند ساماندهی اقدامات اصلاحی مربوط به آن.

به خصوص، به این معنی که تأمین‌کننده باید موارد زیر را انجام دهد:

۱- تأیید انتخاب کارکنان کارفرما یا طرف سومی که ارزیابی یا ممیزی مخاطرات امنیت اطلاعات را به‌منظور صحت‌سنجی انطباق تأمین‌کننده با توافقنامه رابطه با تأمین‌کننده انجام می‌دهد؛

یادآوری – ممکن است، تأمین‌کننده نامزد پیشنهادشده از سوی کارفرما برای انجام ارزیابی یا ممیزی مخاطرات امنیت اطلاعات را به دلایل معتبر رد کند.

۲- کمک به کارفرما در انجام فعالیت‌های زیر که در نتیجه تغییرات مخاطرات امنیت اطلاعات یا عدم تطابق‌های ممیزی حاصل می‌شود:

الف- در نظر گرفتن مجدد جنبه‌های امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده؛ و

ب- تعریف اقدامات اصلاحی که بهتر است در مقیاس زمانی تعریف‌شده برای ادامه فراهم کردن امنیت اطلاعات قابل‌پذیرش برای اطلاعات و سامانه‌های اطلاعاتی کارفرما پیاده‌سازی شود.

ساماندهی این اقدامات اصلاحی باید

	مطابق فرایند ساماندهی اقدامات اصلاحی باشد. ۳) توافق با کارفرما در مورد: i) تغییراتی که بر روی جنبه‌های امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده انجام شود؛ و ii) پیاده‌سازی اقدامات اصلاحی؛ ۴) تأیید توافقنامه به‌روزرسانی‌شده رابطه با تأمین‌کننده.

۷-۴-۴ خروجی‌ها

خروجی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند مدیریت رابطه با تأمین‌کننده توسط هر یک از سازمان‌های زیر تولید شود:

کارفرما	تأمین‌کننده
الف- ارزیابی مخاطرات امنیت اطلاعات و گزارش‌های ممیزی مرتبط با فعالیت‌های پایش و اعمال انطباق.	
در صورت کاربست‌پذیری: ب- ارزیابی مخاطرات امنیت اطلاعات مرتبط با تغییراتی که توسط روش‌های اجرایی مدیریت تغییرات امنیت اطلاعات پوشش داده نشده‌اند؛ پ- گزارش اجرای طرح انتقال؛ ت- تاریخچه تغییرات امنیت اطلاعات و گزارش‌های مربوطه؛ ث- توافقنامه به‌روزرسانی‌شده و تأییدشده رابطه با تأمین‌کننده؛	

یادآوری – توصیه می‌شود، توافقنامه به‌روزرسانی‌شده و تأییدشده رابطه با تأمین‌کننده، برای نگهداری قابلیت ردیابی و یکپارچگی آن در کنار دسترس‌پذیری و محرمانگی، در زمان ذخیره، محافظت شود.
ج- فهرست اقدامات اصلاحی که موردتوافق قرار گرفته و وضعیت جاری آن‌ها(مانند باز، صرف‌نظرشده[1] یا پیاده‌سازی‌شده)

۷-۵ فرایند خاتمه رابطه با تأمین‌کننده

۷-۵-۱ هدف

هدف زیر باید به‌منظور مدیریت موفق امنیت اطلاعات در فرایند خاتمه رابطه با تأمین‌کننده توسط سازمان‌های زیر محقق شود:

کارفرما	تأمین‌کننده
الف-حفاظت از تأمین محصول یا خدمت در مدت خاتمه آن به‌منظور اجتناب از هرگونه تأثیرات امنیت اطلاعاتی، قانونی و مقرراتی بعد از اعلام خاتمه کار؛ ب- خاتمه تأمین محصول یا خدمت با توجه به طرح خاتمه.	

۷-۵-۲ ورودی‌ها

ورودی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند خاتمه رابطه با تأمین‌کننده توسط هر یک از سازمان‌های زیر در نظر گرفته شود:

کارفرما	تأمین‌کننده
الف- تصمیم مدیریتی از سوی کارفرما یا تأمین‌کننده مبنی بر خاتمه تأمین محصول یا خدمت؛ ب- آخرین نسخه در دسترس توافقنامه رابطه با تأمین‌کننده، که باید شامل طرح خاتمه باشد.	
در صورت کاربست‌پذیری: پ- توافقنامه‌های عدم‌افشای[2] موجود که با تأمین‌کنندگان ایجاد شده باشد.	

1 - Withdrawn
2 - Non-disclosure agreement

۷-۵-۳ فعالیت‌ها

کمینه فعالیت‌های زیر باید برای هر یک از سازمان‌های زیر به‌منظور برآورده‌کردن اهداف تعریف‌شده در بند ۷-۵-۷۱-۵-۱ اجرا شود:

کارفرما	تأمین‌کننده
الف- شفاف‌سازی این که آیا انگیزه‌های امنیت اطلاعاتی در تصمیم به خاتمه تأمین محصول یا خدمت وجود دارد، با شخصی که این تصمیم را اتخاذ نموده است؛ در صورت وجود چنین انگیزه‌هایی، شخصی که خاتمه تأمین به وی اعلام شده است باید موارد زیر را انجام دهد: ۱- شناسایی و ارزیابی مخاطرات امنیت اطلاعات مرتبط با انگیزه‌های امنیت اطلاعات داده‌شده به همراه گزینه‌هایی برای تدبیر آن‌ها؛ ۲- حصول اطمینان از این که طرح تدبیر مخاطرات برای مخاطرات شناسایی‌شده و ارزیابی‌شده برای کاهش، تعریف و پیاده‌سازی شده است. **یادآوری** – در صورت نیاز به خاتمه ناگهانی، توصیه می‌شود طرح BCP کارفرما با توجه به اهمیت تأمین محصول یا خدمتی که تصمیم به خاتمه آن گرفته شده است، فعال شود.	
ب- تصمیم‌گیری با تأمین‌کننده در مورد این که آیا تأمین خدمت یا محصول باید لغو شود یا به کارفرما یا تأمین‌کننده دیگری انتقال یابد؛	
پ- تعریف و پیاده‌سازی طرح ارتباط[1] برای اطلاع‌رسانی به کارکنان داخلی و طرف‌های سومی که تحت تأثیر خاتمه تأمین محصول یا خدمت قرار می‌گیرند؛ ت- انتصاب فردی با مسئولیت ساماندهی خاتمه محصول یا خدمت باتوجه به طرح خاتمه؛ ث- حصول اطمینان از وجود موجودی به‌روزرسانی‌شده از دارایی‌هایی که در تأمین محصول یا خدمت استفاده می‌شود؛ ج- انتخاب و توافق با طرف مقابل در مورد دارایی‌هایی با شرایط زیر: ۱- دارایی‌هایی که به کارفرما بازگردانده خواهد شد و یا به تأمین‌کننده دیگری ارسال خواهد شد؛	

1- Communication Plan

۲- به تأمین‌کننده بازگردانده خواهد شد؛

۳- امحا خواهد شد یا توسط کارفرما یا تأمین‌کننده نگهداری خواهد شد.

چ- اجرای خاتمه تأمین محصول یا خدمت با توجه به طرح خاتمه

ح- حصول اطمینان از این که حقوق دسترسی منطقی و فیزیکی که به طرفی مقابلی برای دسترسی و ساماندهی دارایی‌های داخلی لازم برای تأمین محصول یا خدمت اعطا شده است در مدت‌زمان مناسب حذف می‌شود؛ و

خ- توافق با طرف مقابل در مورد دستاوردهای خاتمه محصول یا خدمت تأمین‌شده.

۷-۵-۴ خروجی‌ها

خروجی‌های کمینه زیر باید در زمان اجرای فعالیت‌های امنیت اطلاعات مربوط به فرایند خاتمه رابطه با تأمین‌کننده توسط هر یک از سازمان‌های زیر تولید شود:

کارفرما	تأمین‌کننده
الف- طرح رابطه مرتبط با خاتمه تأمین محصول یا خدمت؛ ب- انتصاب فردی به‌عنوان مسئول خاتمه تأمین محصول یا خدمت؛ پ- موجودی به‌روزرسانی‌شده دارایی‌هایی که در تأمین محصول یا خدمت استفاده شده است؛ ت- گزارش اجرای طرح خاتمه. در صورت کاربست‌پذیری: ث-طرح ارزیابی و تدبیر مخاطرات امنیت اطلاعات در زمینه انگیزه‌های امنیت اطلاعاتی داده‌شده برای خاتمه تأمین محصول یا خدمت؛ ج- گزارش اجرای طرح انتقال؛ چ- گواهینامه‌های امحای دارایی‌ها؛ ح- گزارش در مورد اجرای حق دسترسی‌های منطقی و فیزیکی.	

پیوست الف

(آگاهی‌دهنده)

ارجاعات متقابل میان بندهای ISO/IEC 15288 و بندهای ISO/IEC 27036-2

جدول الف ــ۱ــ ارجاعات متقابل میان بندهای ISO/IEC 15288 و بندهای ISO/IEC 27036-2

بند یا زیربند ISO/IEC 15288	بند یا زیربند ISO/IEC 27036-2
۶-۱ فرایندهای حصول توافق	۶-۱ فرایندهای حصول توافق
۶-۱-۱ فرایند اکتساب	۶-۱-۱ فرایندهای اکتساب
--	۷-۱ فرایند طرح‌ریزی رابطه با تأمین‌کننده
--	۷-۲ فرایند انتخاب رابطه با تأمین‌کننده
--	۷-۳ فرایند حصول توافق با تأمین‌کننده
--	۷-۴ فرایند مدیریت رابطه با تأمین‌کننده
--	۷-۵ فرایند خاتمه رابطه با تأمین‌کننده
۶-۱-۲ فرایند تأمین	۶-۱-۲ فرایند تأمین
--	۷-۲ فرایند انتخاب رابطه با تأمین‌کننده
--	۷-۳ فرایند حصول توافق با تأمین‌کننده
--	۷-۴ فرایند مدیریت رابطه با تأمین‌کننده
--	۷-۵ فرایند خاتمه رابطه با تأمین‌کننده
۶-۲ فرایندهای توانمندساز پروژه سازمانی	۶-۲ فرایندهای توانمندساز پروژه سازمانی
۶-۲-۱ فرایند مدیریت مدل چرخه‌حیات	۶-۲-۱ فرایند مدیریت مدل چرخه حیات
۶-۲-۲ فرایند مدیریت زیرساخت	۶-۲-۲ فرایند مدیریت زیرساخت
۶-۲-۳ فرایند مدیریت سبد پروژه	۶-۲-۳ فرایند مدیریت سبد پروژه
۶-۲-۴ فرایند مدیریت منابع انسانی	۶-۲-۴ فرایند مدیریت منابع انسانی
۶-۲-۵ فرایند مدیریت کیفیت	۶-۲-۵ فرایند مدیریت کیفیت
۶-۳ فرایندهای پروژه	۶-۳ فرایندهای پروژه
۶-۳-۱ فرایند طرح‌ریزی پروژه	۶-۳-۱ فرایند طرح‌ریزی پروژه
۶-۳-۲ فرایند ارزیابی و کنترل پروژه	۶-۳-۲ فرایند ارزیابی و کنترل پروژه
۶-۳-۳ فرایند مدیریت تصمیم	۶-۳-۳ فرایند مدیریت تصمیم

بند یا زیربند ISO/IEC 15288	بند یا زیربند ISO/IEC 27036-2
۶-۳-۴ فرایند مدیریت مخاطرات	۶-۳-۴ فرایند مدیریت مخاطرات
۶-۳-۵ فرایند مدیریت پیکربندی	۶-۳-۵ فرایند مدیریت پیکربندی
۶-۳-۶ فرایند مدیریت اطلاعات	۶-۳-۶ فرایند مدیریت اطلاعات
۶-۳-۷ فرایند سنجش	۶-۳-۷ فرایند سنجش
۶-۴ فرایند فنی	۶-۴ فرایندهای فنی
۶-۴-۱ فرایند تعریف الزامات ذینفع	--
۶-۴-۲ فرایند تحلیل الزامات	--
۶-۴-۳ فرایند طراحی معمارانه	۶-۴-۱ فرایند تعریف الزامات ذینفع
۶-۴-۴ فرایند پیاده‌سازی	--
۶-۴-۵ فرایند یکپارچه‌سازی	--
۶-۴-۶ فرایند صحت‌سنجی	--
۶-۴-۷ فرایند انتقال	--
۶-۴-۸ فرایند اعتبارسنجی	--
۶-۴-۹ فرایند عملیات	--
۶-۴-۱۰ فرایند نگهداری	--
۶-۴-۱۱ فرایند امحا	

پیوست ب

(آگاهی‌دهنده)

ارجاعات متقابل میان بندهای ISO/IEC 27036-2 و کنترل‌های ISO/IEC 27002

جدول ب ـ۱ـ ارجاعات متقابل میان بندهای ISO/IEC 27036-2 و کنترل‌های ISO/IEC 27002

بند یا زیربند ISO/IEC 27036-2	بند یا زیربند ISO/IEC 27002
۶-۱ فرایندهای حصول توافق	۵-خط‌مشی امنیتی ۶- سازمان امنیت اطلاعات ۱۵- روابط با تأمین‌کننده ۱۸- انطباق
۶-۱-۱فرایندهای اکتساب	به نگاشت ۶-۱ مراجعه شود
۶-۱-۲ فرایند تأمین	به نگاشت ۶-۱ مراجعه شود
۶-۲ فرایندهای توانمندساز پروژه سازمانی	فرایندهای منفرد برای نگاشت‌های خاص را مشاهده کنید
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 ۱۴- اکتساب، بهبود و نگهداری سامانه‌های اطلاعاتی ۱۶- مدیریت رخدادهای امنیت اطلاعات ۱۷- جنبه‌های امنیت اطلاعات مدیریت تداوم 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

بند یا زیربند ISO/IEC 27036-2	بند یا زیربند ISO/IEC 27002
۶-۳ فرایندهای پروژ	فرایندهای منفرد برای نگاشت‌های خاص را مشاهده کنید.
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 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	هیچ‌کدام
۶-۴ فرایندهای فنی	فرایندهای منفرد برای نگاشت‌های خاص را مشاهده کنید.
۶-۴-۱ فرایند تعریف الزامات ذینفع	هیچ‌کدام
۷-۱ فرایند طرح‌ریزی رابطه با تأمین‌کننده	۱۵-۱روابط با تأمین‌کننده
	هیچ‌کدام
۷-۲ فرایند انتخاب رابطه با تأمین‌کننده	۱۵-۱ امنیت اطلاعات در روابط با تأمین‌کننده
۷-۳ فرایند حصول توافق با تأمین‌کننده	۱۵-۲ مدیریت تحویل خدمات تأمین‌کننده
۷-۴ فرایند مدیریت رابطه با تأمین‌کننده	هیچ‌کدام

پیوست پ

(آگاهی‌دهنده)

اهداف بندهای ۶ و ۷

جدول پ ـ۱ـ اهداف بندهای ۶ و ۷

کارفرما
۶-۱-۱ فرایند اکتساب الف- ایجاد راهبرد رابطه با تأمین‌کننده که: ۱- بر مبنای تحمل‌پذیری مخاطرات امنیت اطلاعات از سوی کارفرما باشد؛ ۲- مبنای امنیت اطلاعات برای استفاده در زمان طرح‌ریزی، آماده‌سازی، مدیریت و خاتمه تدارک محصول یا خدمت را تعریف کند.
۶-۱-۲فرایند تأمین هیچ‌کدام
۶-۲-۱فرایند مدل چرخه‌ی حیات الف- کارفرما و تأمین‌کننده باید فرایند مدیریت مدل چرخه‌حیات را در زمان مدیریت امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند.
۶-۲-۲ فرایند مدیریت زیرساخت الف- فراهم کردن زیرساخت توانمندساز به‌منظور پشتیبانی سازمان در زمینه مدیریت زیرساخت امنیت اطلاعات در روابط با تأمین‌کننده.
۶-۲-۳ فرایند مدیریت سبد پروژه الف- ایجاد فرایندی برای در نظرگرفتن امنیت اطلاعات و استلزام‌ها و وابستگی‌های کلی کسب‌وکار مربوط به هر پروژه، برای آن دسته از پروژه‌هایی که تأمین‌کنندگان یا کارفرمایان در آن درگیر هستند.
۶-۲-۴ فرایند مدیریت منابع انسانی الف- حصول اطمینان از این که کارفرما و تأمین‌کننده دارای نیروهای انسانی هستند که دارای شایستگی‌های منطبق با نیازهای امنیت اطلاعات در روابط با تأمین‌کننده هستند و شایستگی‌های آن‌ها در سطح مورد انتظار به‌صورت منظم نگهداری می‌شود.
۶-۲-۵ فرایند مدیریت کیفیت الف- کارفرما و تأمین‌کننده باید فرایند مدیریت کیفیتی را در زمان مدیریت امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند.

۶-۳-۱ فرایند طرح‌ریزی پروژه

الف- ایجاد فرایند طرح‌ریزی پروژه با پرداختن به امنیت اطلاعات روابط با تأمین‌کننده.

۶-۳-۲ فرایند کنترل و ارزیابی پروژه

الف- کارفرما و تأمین‌کننده باید فرایند کنترل و ارزیابی پروژه را در زمان مدیریت امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند.

۶-۳-۳ فرایند مدیریت تصمیم

الف- کارفرما و تأمین‌کننده باید مدیریت تصمیم را در زمان مدیریت امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند.

۶-۳-۴ فرایند مدیریت مخاطرات

الف- پرداختن مداوم به مخاطرات امنیت اطلاعات در روابط با تأمین‌کننده و در چرخه حیات آن‌ها شامل بررسی مجدد آن‌ها به‌صورت دوره‌ای یا در زمان وقوع تغییرات کسب‌وکار، قانونی، مقرراتی، معماری، خط‌مشی‌ها و قراردادی

۶-۳-۵ فرایند مدیریت پیکربندی

الف- در صورتی‌که قابل کاربرد باشد، کارفرما و تأمین‌کننده باید فرایند مدیریت پیکربندی را در زمان اجرای امنیت اطلاعات در روابط با تأمین‌کننده ایجاد کنند.

۶-۳-۶ فرایند مدیریت اطلاعات

الف- کارفرما و تأمین‌کننده باید فرایند مدیریت اطلاعات را با در نظر گرفتن حساسیت اطلاعاتی که می‌تواند در مدت روابط با تأمین‌کننده تبادل شود، ایجاد کند.

۶-۳-۷ فرایند مدیریت سنجش

الف- جمع‌آوری، تحلیل، و گزارش سنجه‌های امنیت اطلاعات مرتبط با تدارک یا تأمین محصول یا خدمت به‌منظور نمایش بلوغ امنیت اطلاعات در روابط با تأمین‌کننده و به‌منظور پشتیبانی از مدیریت اثربخش فرایندها.

۶-۴-۱ فرایند طراحی معمارانه

الف- ایجاد چارچوب فنی برای تدارک مداوم محصول یا خدمت که هدف روابط با تأمین‌کننده را برآورده کند.

۷-۱ فرایند طرح‌ریزی رابطه با تأمین‌کننده

الف- ایجاد طرح رابطه با تأمین‌کننده‌ای که تصمیمات پذیرفته‌شده توسط مدیریت به‌منظور آغاز تدارک محصول یا خدمت و همچنین ملاحظات امنیت اطلاعات مربوط به اکتساب را مستندسازی کند.

۷-۷۲-۲ فرایند انتخاب تأمین‌کننده

الف- انتخاب تأمین‌کننده‌ای که امنیت اطلاعات کافی را برای محصول یا خدمتی که ممکن است تدارک شود، فراهم کند.

Error! Reference source not found.-۳-۷ فرایند حصول توافق با تأمین‌کننده

الف- ایجاد و توافق بر سر توافقنامه رابطه با تأمین‌کننده که به موارد زیر بپردازد:

۱- نقش‌ها و مسئولیت‌های امنیت اطلاعات کارفرما و تأمین‌کننده؛

۲- فرایند انتقال در مواقعی که محصول یا خدمت پیش‌ازاین توسط شخصی به غیر از تأمین‌کننده بهره‌برداری یا ساخته شده است؛

۳- مدیریت تغییر امنیت اطلاعات؛

۴- مدیریت رخدادهای امنیت اطلاعات؛

۵-پایش و اعمال انطباق؛

۶- فرایند خاتمه.

۴-۷۴-۷ فرایند مدیریت رابطه با تأمین‌کننده

الف- نگهداری امنیت اطلاعات در مدت‌زمان اجرای رابطه با تأمین‌کننده در انطباق با توافقنامه رابطه با تأمین‌کننده و به خصوص با در نظر گرفتن موارد زیر:

۱- انتقال تأمین محصول یا خدمت پیش‌ازاین توسط کارفرما یا تأمین‌کننده دیگری بهره‌برداری یا ساخته شده باشد.

۲- آموزش کارکنانی که تحت تأثیر الزامات امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده قرار گرفته‌اند؛

۳- مدیریت تغییرات و رخدادهایی که می‌تواند بر روی تأمین محصول یا خدمت تأثیرگذار باشد؛

۴- پایش و اعمال انطباق تأمین‌کننده با شرایط امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده.

۵-۷۵-۷ فرایند خاتمه رابطه با تأمین‌کننده

الف-حفاظت از تأمین محصول یا خدمت در مدت خاتمه آن به‌منظور اجتناب از هرگونه تأثیرات امنیت اطلاعاتی، قانونی و مقرراتی بعد از اعلام خاتمه؛

ب- خاتمه تأمین محصول یا خدمت با توجه به طرح خاتمه.

تأمین‌کننده

۱-۱-۶ فرایند اکتساب

هیچ‌کدام

۲-۱-۶ فرایند تأمین

الف- ایجاد راهبرد رابطه با تأمین‌کننده که:

۱- بر مبنای تحمل‌پذیری مخاطرات امنیت اطلاعات از سوی تأمین‌کننده باشد؛

۲- مبنای امنیت اطلاعات برای استفاده در زمان طرح‌ریزی، آماده‌سازی، مدیریت و خاتمه تدارک محصول یا خدمت را تعریف کند.

۶-۲-۱ فرایند مدل چرخه‌ی حیات

الف- کارفرما و تأمین‌کننده باید فرایند مدیریت مدل چرخه حیات را در زمان مدیریت امنیت اطلاعات در روابط تأمین‌کننده ایجاد کنند.

۶-۲-۲ فرایند مدیریت زیرساخت

الف- فراهم کردن زیرساخت توانمندساز به‌منظور پشتیبانی سازمان در زمینه مدیریت زیرساخت امنیت اطلاعات در روابط با تأمین‌کننده.

۶-۲-۳ فرایند مدیریت سبد پروژه

الف- ایجاد فرایندی برای در نظر گرفتن امنیت اطلاعات و استلزام‌ها و وابستگی‌های کلی کسب‌وکار مربوط به هر پروژه، برای آن دسته از پروژه‌هایی که تأمین‌کنندگان یا کارفرمایان در آن درگیر هستند.

۶-۲-۴ فرایند مدیریت منابع انسانی

الف- حصول اطمینان از این که کارفرما و تأمین‌کننده دارای نیروهای انسانی هستند که دارای شایستگی‌های منطبق با نیازهای امنیت اطلاعات در روابط با تأمین‌کننده هستند و شایستگی‌های آن‌ها در سطح مورد انتظار به‌صورت منظم نگهداری می‌شود.

۶-۲-۵ فرایند مدیریت کیفیت

الف- کارفرما و تأمین‌کننده باید فرایند مدیریت کیفیتی را در زمان مدیریت امنیت اطلاعات در روابط تأمین‌کننده ایجاد کنند.

۶-۳-۱فرایند طرح‌ریزی پروژه

الف- ایجاد فرایند طرح‌ریزی پروژه با پرداختن به امنیت اطلاعات روابط با تأمین‌کننده.

۶-۳-۲ فرایند کنترل و ارزیابی پروژه

الف- کارفرما و تأمین‌کننده باید فرایند کنترل و ارزیابی پروژه را در زمان مدیریت امنیت اطلاعات در روابط تأمین‌کننده ایجاد کنند.

۶-۳-۳ فرایند مدیریت تصمیم

الف- کارفرما و تأمین‌کننده باید مدیریت تصمیم را در زمان مدیریت امنیت اطلاعات در روابط تأمین‌کننده ایجاد کنند.

۶-۳-۴ فرایند مدیریت مخاطرات

الف- پرداختن مداوم به مخاطرات امنیت اطلاعات در روابط با تأمین‌کننده و در چرخه حیات آن‌ها شامل بررسی مجدد آن‌ها به‌صورت دوره‌ای یا در زمان وقوع تغییرات کسب‌وکار، قانونی، مقرراتی، معماری، خط‌مشی‌ها و قراردادی

۶-۳-۵فرایند مدیریت پیکربندی

الف- درصورتی‌که قابل کاربرد باشد، کارفرما و تأمین‌کننده باید فرایند مدیریت پیکربندی را در زمان اجرای امنیت اطلاعات در روابط تأمین‌کننده ایجاد کنند.

۶-۳-۶ فرایند مدیریت اطلاعات

الف- کارفرما و تأمین‌کننده باید فرایند مدیریت اطلاعات را با در نظر گرفتن حساسیت اطلاعاتی که می‌تواند در مدت روابط تأمین‌کننده تبادل شود، ایجاد کند.

۶-۳-۷فرایند مدیریت سنجش

الف- جمع‌آوری، تحلیل و گزارش سنجه‌های امنیت اطلاعات مرتبط با تدارک یا تأمین محصول یا خدمت به‌منظور نمایش بلوغ امنیت اطلاعات در روابط با تأمین‌کننده و به‌منظور پشتیبانی از مدیریت اثربخش فرایندها.

۶-۴-۱فرایند طراحی معمارانه

الف- ایجاد چارچوب فنی برای تدارک مداوم محصول یا خدمت که هدف روابط با تأمین‌کننده را برآورده کند.

۷۷-۱ فرایند طرح‌ریزی رابطه با تأمین‌کننده

هیچ‌کدام

۷-۲فرایند انتخاب تأمین‌کننده

الف- پاسخ به سند اسناد مناقصه کارفرما با در نظر گرفتن مخاطرات امنیت اطلاعات مربوط به محصول یا خدمتی که قصد تأمین آن وجود دارد و الزامات امنیت اطلاعات اسناد مناقصه کارفرما (مانند ITT، RFP)

Error! Reference source not found. فرایند حصول توافق با تأمین‌کننده

الف- ایجاد و توافق بر سر توافقنامه رابطه با تأمین‌کننده که به موارد زیر بپردازد:

۱- نقش‌ها و مسئولیت‌های امنیت اطلاعات کارفرما و تأمین‌کننده؛

۲- فرایند انتقال در مواقعی که محصول یا خدمت پیش‌ازاین توسط شخصی به غیر از تأمین‌کننده بهره‌برداری یا ساخته شده است؛

۳- مدیریت تغییر امنیت اطلاعات؛

۴- مدیریت رخدادهای امنیت اطلاعات؛

۵-پایش و اعمال انطباق؛

۶- فرایند خاتمه.

۷-۴ فرایند مدیریت رابطه با تأمین‌کننده

الف- نگهداری امنیت اطلاعات در مدت‌زمان اجرای رابطه با تأمین‌کننده در انطباق با توافقنامه رابطه با تأمین‌کننده و به

خصوص با در نظر گرفتن موارد زیر:

۱- پشتیبانی از کارفرما در انتقال تأمین محصول یا خدمتی که پیش از این توسط کارفرما یا تأمین‌کننده دیگری بهره‌برداری یا ساخته شده باشد.

۲- آموزش کارکنانی که تحت تأثیر الزامات امنیت اطلاعات تعریف‌شده در توافقنامه رابطه با تأمین‌کننده قرار گرفته‌اند؛

۳- مدیریت تغییرات و رخدادهایی که می‌تواند بر روی تأمین محصول یا خدمت تأثیرگذار باشد؛

۴- پشتیبانی از کارفرما در فعالیت‌های پایش و اعمال انطباق.

۷-۵ فرایند خاتمه رابطه با تأمین‌کننده

الف-حفاظت از تأمین محصول یا خدمت در مدت خاتمه آن به‌منظور اجتناب از هرگونه تأثیرات امنیت اطلاعاتی، قانونی و مقرراتی بعد از اعلام خاتمه؛

ب- خاتمه تأمین محصول یا خدمت با توجه به طرح خاتمه.

کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۱۶۰۳۴: سال ۱۳۹۱، مهندسی سامانه‌ها و نرم‌افزار- فرایندهای چرخه حیات سامانه

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

[۳] استاندارد ملی ایران شماره ۲۷۰۳۱: سال ۱۳۹۱، فناوری اطلاعات -فنون امنیتی -راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به‌منظور تداوم کسب‌وکار

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

[۵] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، فناوری اطلاعات – فنون امنیتی – سامانه(سیستم) مدیریت امنیت اطلاعات – الزامات

[۶] استاندارد ملی ایران شماره ۲۷۰۳۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات

[7] ISO 22313, Societal security — Business continuity management systems — Guidance

[8] ISO 22301, Societal security — Business continuity management systems --- Requirements

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

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