INSO-ISO-IEC

27036-1

1st. Edition

2015

Identical with
ISO/IEC 27036-1:
2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران-ایزو-
آی ای سی
۲۷۰۳۶-۱
چاپ اول
۱۳۹۳

فناوری اطلاعات- فنون امنیتی-امنیت اطلاعات برای روابط تأمین‌کننده- قسمت ۱: مرور کلی و مفاهیم

Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts

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 ۱: مرور کلی و مفاهیم »

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**

آشنایی با سازمان ملی استاندارد ایران **Error! Bookmark not defined.**
کمیسیون فنی تدوین استاندارد ج
پیش‌گفتار و
۱ هدف و دامنه کاربرد ۱
۲ مراجع الزامی ۱
۳ اصطلاحات و تعاریف ۱
۴ کوته‌نوشت‌ها ۵
۵ تعریف مسئله و مفاهیم کلیدی ۵
۵-۱ انگیزه‌های ایجاد روابط تأمین‌کننده ۵
۵-۲ انواع روابط تأمین‌کننده ۶
۵-۲-۱ روابط تأمین‌کننده برای محصولات ۶
۵-۲-۲ روابط تأمین‌کننده برای خدمات ۶
۵-۲-۳ زنجیره تأمین ICT ۷
۵-۲-۴ رایانش ابری ۸
۵-۳ مخاطرات امنیت اطلاعات در روابط تأمین‌کننده و تهدیدهای مرتبط با آن ۹
۵-۴ مدیریت مخاطرات امنیت اطلاعات در روابط تأمین‌کننده ۱۳
۵-۵ ملاحظات زنجیره تأمین ICT ۱۴
۶ ساختار کلی ISO/IEC 27036 و مرور کلی ۱۵
۶-۱ هدف و ساختار ۱۵
۶-۲ مرور کلی قسمت ۱: مرور کلی و مفاهیم ۱۵
۶-۳ مرور کلی قسمت ۲: الزامات ۱۶
۶-۴ مرور کلی قسمت ۳: راهنماهایی برای امنیت زنجیره تأمین فناوری اطلاعات و ارتباطات(ICT) در روابط تأمین‌کننده ۱۶
۶-۵ مرور کلی قسمت ۴: راهنماهایی برای امنیت خدمات ابری ۱۷

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی -امنیت اطلاعات برای روابط تأمین‌کننده–قسمت ۱: مرور کلی و مفاهیم» که پیش نویس 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 ۹۳/۱۱/۲۹ 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 می شود .

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

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

ISO/IEC 27036-1: 2014, Information Technology — Security Techniques — Information Security for Supplier Relationships— Part 1: Overview and concepts

فناوری اطلاعات -فنون امنیتی- امنیت اطلاعات برای روابط تأمین‌کننده

قسمت ۱: مرور کلی و مفاهیم

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین مرور کلی راهنمای در نظر گرفته‌شده برای کمک به سازمان‌ها در مورد ایمن‌سازی اطلاعات و سامانه‌های اطلاعاتی در زمینه روابط تأمین‌کننده است. این استاندارد، همچنین، مفاهیمی را که به تفصیل در قسمت‌های دیگر این استاندارد توصیف شده است معرفی می‌کند. این استاندارد جنبه‌هایی از هر دو گروه کارفرمایان و تأمین‌کنندگان 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.

در صورتی که به مدرکی با بیان تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر 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 مورد نظر است.

استفاده از مرجع زیر[۱] برای این استاندارد الزامی است:

2-1 ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

۳ اصطلاحات و تعاریف

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

۳-۱

کارفرما[۲]

ذینفعی که محصول یا خدمتی را از شخص[۳] دیگری تدارک می‌بیند.

یادآوری- تدارکات می‌تواند شامل تبادل پول باشد یا نباشد.

---

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

2- Acquierer

3- Party

[استاندارد ملی ایران شماره ۱۶۳۰۴ : سال ۱۳۹۱، بند ۴-۱]

۲-۳

اکتساب

فرآیند به دست آوردن محصول یا خدمت یک سامانه است.

[استاندارد ملی ایران شماره ۱۶۳۰۴ : سال ۱۳۹۱، بند ۴-۲]

۳-۳

توافقنامه[1]

تصدیق متقابل قواعد و شرایط انجام یک رابطه کاری است.

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

۴-۳

چرخه حیات[2]

تکامل یک سامانه، محصول، خدمت، پروژه یا دیگر هستارهای انسان ساخته از مرحله‌ی طراحی مفهومی تا برچیدن، چرخه حیات نامیده می‌شود.

[استاندارد ملی ایران شماره ۱۶۳۰۴ : سال ۱۳۹۱، بند ۴-۱۱]

۵-۳

پایین‌دست[3]

اداره کردن فرآیندها و جابجایی محصولات و خدمات، بعد از هستاری است که حفاظت از محصولات و مسئولیت خدمات را در زنجیره تأمین بر عهده دارد.

[ISO 28001:2007 بند ۳ـ۱۰]

۶-۳

برون‌سپاری[4]

اکتساب خدمات (با محصولات یا بدون آن‌ها) در پشتیبانی از یک کارکرد کسب‌وکار به‌منظور انجام فعالیت‌ها با استفاده از منابع تأمین‌کننده به‌جای منابع کارفرما است.

1- Agreement
2- Life cycle
3- Downstream
4- Outsourcing

۷-۳

فرایند

مجموعه‌ای از فعالیت‌های متصل یا مرتبط به هم است که ورودی‌ها را به خروجی‌ها تبدیل می‌کند.

[استاندارد ملی ایران شماره ۹۰۰۰ : سال ۱۳۸۷]

۸-۳

ذی‌نفع[1]

فرد یا سازمانی با گرایش به یک دارایی در رابطه تأمین‌کننده است.

یادآوری- در این استاندارد ملی، دارایی به معنای اطلاعات مربوط به محصولات و خدمات به کار می‌رود.

۹-۳

تأمین‌کننده[2]

سازمان یا فردی است که برای تأمین یک محصول یا خدمت با کارفرما وارد توافق می‌شود.

یادآوری ۱- اصطلاحات دیگری که به‌صورت متداول برای تأمین‌کننده استفاده می‌شوند عبارت‌اند از پیمانکار[3]، تولیدکننده و فروشنده.

یادآوری ۲- کارفرما و تأمین‌کننده می‌توانند قسمتی از یک سازمان مشابه باشند.

یادآوری ۳- انواع تأمین‌کنندگان شامل سازمان‌هایی است که اجازه مذاکرات توافق با یک کارفرما را می‌دهند و سازمان‌هایی که اجازه مذاکره در مورد توافق را نمی‌دهند، مانند توافق امتیاز کاربر نهایی، شرایط استفاده، یا حق نشر محصولات یا انتشار دارایی‌های معنوی.[استاندارد ملی ایران شماره ۱۶۳۰۴ : سال ۱۳۹۱، بند ۴-۳۰]

۱۰-۳

ارتباط تأمین‌کننده[4]

توافق یا توافق‌هایی است که بین کارفرما و تأمین‌کننده برای عرضه محصولات یا خدمات و درک مزایای کسب‌وکار منعقد می‌شود.

۱۱-۳

زنجیره تأمین[5]

مجموعه‌ای از سازمان‌ها با مجموعه پیوندیافته از منابع و فرایندها است که هر یک از آن‌ها نقش یک کارفرما،

1- Stakeholder
2- Supplier
3-Contractor
4- Supplier relationship
5- Supply chain

تأمین‌کننده و یا هر دوی آن‌ها را در قالب روابط متوالی که به‌وسیله قرار دادن یک سفارش یا توافق یا دیگر انواع توافق‌های تأمین منبع بر عهده می‌گیرند.

یادآوری ۱- یک زنجیره تأمین می‌تواند شامل فروشندگان، مؤسسات تولیدی، تأمین‌کنندگان آماد[1]، مراکز توزیع، توزیع‌کنندگان، عمده‌فروشان و دیگر سازمان‌هایی شود که در تولید، پردازش، طراحی و توسعه و اداره و تحویل خدمات درگیر هستند.

یادآوری ۲- دید زنجیره تأمین با توجه به موقعیت کارفرما نسبی است.

[ISO 28001:2007 بند ۳ـ۲۴]

۱۲-۳

سامانه[2]

ترکیب مؤلفه‌های تعامل گری است که به‌منظور دستیابی به یک یا چند هدف اعلام‌شده، سازمان یافته است.

یادآوری ۱- یک سامانه می‌تواند به‌عنوان محصولات یا خدماتی که تولید می‌کند در نظر گرفته شود.

یادآوری ۲- در عمل، تفسیر معنای سامانه اغلب با استفاده از یک نام ارتباط‌دهنده برای مثال سامانه هواپیما شفاف‌سازی می‌شود. در حالتی دیگر، واژه‌ی « سامانه» ممکن است به‌سادگی با یک مترادف وابسته به زمینه‌ی مفهومی[3] جایگزین شود. به‌عنوان‌مثال، هواپیما؛ در حالی که این امر می‌تواند از دیدگاه اصول سامانه، ایجاد ابهام کند.

[استاندارد ملی ایران شماره ۱۶۳۰۴ : سال ۱۳۹۱، بند ۴-۳۱]

۱۳-۳

اعتماد [4]

ارتباط میان دو یا چند هستار است که شامل مجموعه‌ای از فعالیت‌ها و یک سیاست امنیتی است که در آن‌ها مؤلفه X به مؤلفه Y اعتماد می‌کند اگر و تنها اگر X مطمئن باشد که Y به صورتی خوش‌تعریف (با توجه به فعالیت‌ها) رفتار خواهد کرد که سیاست امنیتی داده‌شده نقض نشود.

[استاندارد ملی ایران شماره ۱۳۸۸۸ : سال ۱۳۸۹]

۱۴-۳

بالادست[5]

اداره کردن فرآیندها و جابه‌جایی محصولات و خدمات، قبل از هستاری است که حفاظت از محصولات و مسئولیت خدمات را در زنجیره تأمین بر عهده دارد.

[ISO 28001:2007 بند ۳ـ۲۷]

1- logistics
2- System
3- Context-dependent synonym
4- Trust
5- Upstream

۱۵-۳

مشاهده‌پذیری[1]

ویژگی یک سامانه یا فرایند است که مؤلفه‌ها و فرایندهای سامانه را قابل مستندسازی کرده و برای پایش و بازرسی دسترس‌پذیر می‌سازد.

۴ کوته‌نوشت‌ها

API	واسط برنامه‌نویسی برنامه کاربردی — Application Programming Interface
ASP	ارائه‌دهنده خدمت برنامه کاربردی — Application Service Provider
BCP	طرح تداوم کسب‌وکار — Business Continuity Plan(ning)
BPaaS	فرایند کسب‌وکار به‌عنوان خدمت — Business Process as a Service
IaaS	زیرساخت به‌عنوان خدمت — Infrastructure as a Service
ICT	فناوری اطلاعات و ارتباطات — Information and Communication Technology
PaaS	بستر به‌عنوان خدمت — Platform as a Service
R&D	تحقیق و توسعه — Research & Development
SaaS	نرم‌افزار به‌عنوان خدمت — Software as a Service

۵ تعریف مسئله و مفاهیم کلیدی

۱-۵ انگیزه‌های ایجاد روابط تأمین‌کننده

سازمان‌ها به‌طور معمول به دلایل مختلفی اقدام به شکل‌دهی و/یا حفظ روابط تأمین‌کننده برای بهره‌مندی از مزایایی که آن‌ها می‌توانند فراهم کنند، می‌کنند:

الف) تمرکز منابع داخلی بر کارکرد اصلی کسب‌وکار که می‌تواند موجب کاهش هزینه و بهبود بازگشت سرمایه شود(مانند برون‌سپاری خدمات ICT)

ب) اکتساب شایستگی بسیار تخصصی یا کوتاه‌مدت که سازمان پیش از این فاقد آن بوده است (مانند به خدمت گرفتن یک مؤسسه تبلیغاتی)، به‌منظور دستیابی به اهداف کسب‌وکار مورد نظر.

پ) اکتساب تجهیزات یا خدمات ICT جدید (مانند رایانه‌های کیفی[2]، چاپگرها، کارسازها[3]، رهیاب‌ها[4]،

1- Visibility
2- Laptops
3- Servers
4- Routers

برنامه‌های کاربردی نرم‌افزاری، ظرفیت حافظه، اتصال‌دهندگی شبکه[1]، خدمات مدیریت ICT و غیره) یا جایگزینی آن‌ها که بهره‌وری نیروی کار و پاسخگویی به دیگر نیازهای رایانشی کسب‌وکار را به همراه دارد.

تأمین‌کنندگان می‌توانند چندین محصول یا خدمت شامل برون‌سپاری فناوری اطلاعات، خدمات حرفه‌ای، خدمات پایه(خدمت نگهداشت تجهیزات، خدمت نگهبان‌ها امنیتی، تصفیه و ارائه خدمات و غیره)، خدمات رایانش ابری، فناوری اطلاعاتی و ارتباطاتی(ICT)، مدیریت دانش، R&D، تولید، آماد، خدمات مراقبت از سلامت، خدمات اینترنت، و بسیاری دیگر را فراهم نمایند.

۵-۲ انواع روابط تأمین‌کننده

۵-۲-۱ روابط تأمین‌کننده برای محصولات

هنگامی‌که کارفرمایی وارد یک رابطه تأمین‌کننده برای محصولات می‌شود، به‌طور معمول محصولاتی را با مشخصات توافق‌شده برای یک دوره از پیش‌مشخص‌شده، به‌منظور تولید محصولات مورد نیاز خریداری می‌کند.

تأمین‌کننده می‌تواند در زمان ارائه و پشتیبانی محصول به اطلاعات کارفرما دسترسی داشته باشد که این ممکن است منجر به مخاطرات امنیت اطلاعات برای اطلاعات کارفرما شود. ممکن است کارفرما قصد کنترل اجزای فرایندهای تولید تأمین‌کننده را به‌منظور نگهداشت کیفیت محصولات و همچنین کاهش مخاطرات امنیت اطلاعات مشتق‌شده از آسیب‌پذیری‌ها، نواقص یا دیگر خرابی‌ها به‌منظور برآورده کردن نیازمندی‌ها داشته باشد. این کار در مقابل می‌تواند مخاطرات امنیت اطلاعات را به تأمین‌کننده تحمیل کند چرا که کارفرما می‌تواند در زمان کنترل اجزای فرآیندهای تأمین‌کننده به اطلاعات آن دسترسی داشته باشد.

علاوه بر آن، ممکن است کارفرما بخواهد در مورد مشخصه محصولات به‌وسیله پایش یا ممیزی فرآیندهای تولید یا الزام تأمین‌کننده به کسب یک مجوز مستقل برای نشان دادن وجود عملکرد خوب و فرآیندهای لازم اطمینان حاصل کند. ضروری است الزامات اطمینان‌بخشی میان کارفرما و تأمین‌کننده مورد توافق قرار گیرند.

۵-۲-۲ روابط تأمین‌کننده برای خدمات

هنگامی‌که کارفرمایی خدماتی را خریداری می‌کند، تأمین‌کننده به‌طور عموم به اطلاعات کارفرما دسترسی دارد. این مسئله موجب مخاطرات بالقوه امنیتی برای کارفرما می‌شود. در مورد برون‌سپاری فرایند کسب‌وکار مانند بازاریابی، عملیات مرکز تماس یا زیرساخت‌های ICT سازمان، بخش قابل توجهی از اطلاعات بحرانی کسب‌وکار می‌تواند تحت مدیریت تأمین‌کننده قرار گیرد. انواع دیگر خدمات مانند خدمات غذایی یا نظافت به‌طور معمول دسترسی محدودی به اطلاعات کارفرما دارند.

تحویل برخی از خدمات نیازمند آن است که اطلاعات در داخل محل کارفرما قرار گرفته و تأمین‌کننده، در محل یا از راه دور به آن دسترسی داشته باشد. در موارد دیگر، اطلاعات کارفرما در محل تأمین‌کننده قرار می‌گیرد. این شرایط خاص می‌تواند بر انتخاب کنترل‌های قابل‌اعمال بر روی کارفرما یا تأمین‌کننده تأثیر

1- Network connectivity

داشته باشد. برای مشاهده نمونه‌هایی درباره آن‌که چگونه مکان می‌تواند بر روی دسترسی تأمین‌کننده به اطلاعات کارفرما تأثیرگذار باشد، جدول ۲ مشاهده شود.

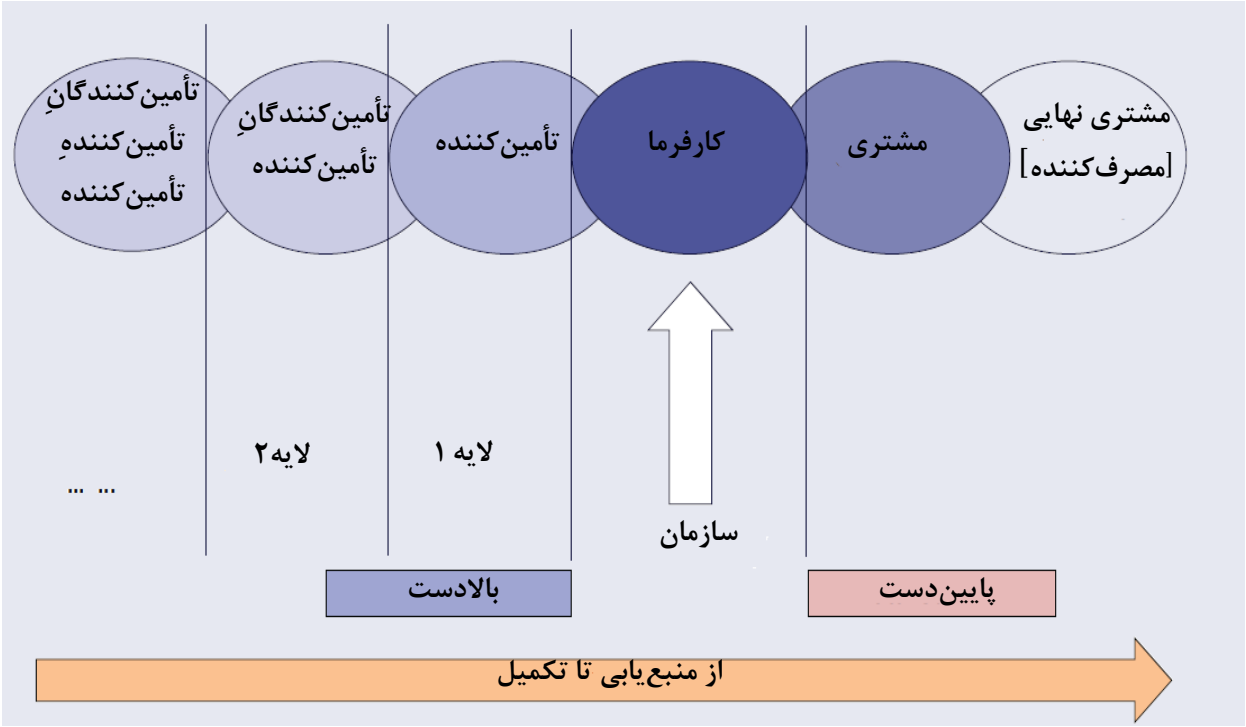
هنگام اکتساب خدمات، کارفرما باید قوانینی در رابطه با چگونگی کنترل دسترسی تأمین‌کننده به اطلاعات کارفرما وضع کند. ممکن است کارفرما به‌منظور کاهش مخاطرات امنیتی، تمایل به کنترل کیفیت خدمت، مانند توانایی برآورده کردن الزامات دسترس‌پذیری در طول زمان داشته باشد. یک توافق سطح خدمت[1] روشی عمومی برای توافق بر کیفیت خدمات است. برای تأمین‌کننده، یک توافق سطح خدمت می‌تواند ابزاری در ارتباط با چگونگی ارضای انتظارات کیفیتی کارفرما باشد.

ممکن است کارفرما به داشتن تضمین در رابطه با کیفیت خدمت به‌وسیله پایش یا ممیزی فرآیندهای خدمت‌رسانی تأمین‌کننده یا الزام کردن تأمین‌کننده به کسب گواهی برای نمایش عملیات خوب یا فرآیندهای لازم تمایل داشته باشد. این الزامات تضمین نیز باید مورد توافق اشخاص قرار گیرد.

۵-۲-۳ زنجیره تأمین ICT

زنجیره تأمین ICT مجموعه‌ای از سازمان‌ها با یک مجموعه پیوندیافته از منابع و فرایندهایی است که روابط متوالی تأمین‌کننده از محصولات و خدمات ICT را شکل می‌دهند. محصول یا خدمت ICT می‌تواند از مؤلفه‌ها، منابع و فرآیندهای تولیدی یک تأمین‌کننده تشکیل شده باشد که آن‌ها نیز می‌توانند به‌صورت کامل یا بخشی توسط یک تأمین‌کننده دیگر تولید شده باشند. همچنین، خدمت ICT ممکن است به‌صورت کامل از چندین تأمین‌کننده تهیه شود. همان‌گونه که در شکل ۱ نشان داده شده است، یک سازمان در یک زنجیره تأمین نسبت به سازمان بالادست کارفرما و نسبت به سازمان پایین‌دست تأمین‌کننده است. سازمان بالادست مجاور، به‌طور معمول از نظر سازمانی که خدمات و محصولات را برای آن فراهم می‌کند، مشتری خوانده می‌شود. مشتری انتهای زنجیره تأمین ICT مشتری انتهایی یا مصرف‌کننده نامیده می‌شود. به‌صورت عمومی، مشتری نهایی کنترل محدودی بر روی الزامات امنیت اطلاعات تأمین‌کنندگان مستقیم داشته و هیچ کنترلی بر روی الزامات امنیت اطلاعات فراتر از تأمین‌کننده مستقیم ندارد.

1- Service Level Agreement



شکل ۱- روابط زنجیره تأمین

کارفرمایان و تأمین‌کنندگان در سراسر زنجیره تأمین ICT مخاطرات امنیت اطلاعات مرتبط با روابط منفرد تأمین‌کننده را از محصولات و خدمات به ارث می‌برند(به بخش‌های ۵-۲-۱ و ۵-۲-۳ مراجعه شود). با این وجود، مدیریت این مخاطرات امنیت اطلاعات از طریق ارتباط، پایش و اعمال امنیت اطلاعات در سراسر زنجیره تأمین، با توجه به مشاهده‌پذیری و دسترسی محدود به تأمین‌کنندگانِ تأمین‌کننده چالش‌برانگیز است

۵-۲-۴ رایانش ابری

رایانش ابری شکلی از یک رابطه تأمین‌کننده است که در آن ممکن است یک خدمت رایانش ابری به‌صورت کامل از طریق چندین تأمین‌کننده فراهم شود. هدف رایانش ابری توانمندسازی رایانش مبتنی بر سودمندی یا بر مبنای استفاده و خدمات ذخیره‌سازی و قابلیت‌های مبتنی بر الزامات کسب‌وکار برای انتظارات مقیاس‌پذیری، دسترس‌پذیری و قابلیت ارتجاعی از خدمات است. در یک خدمت رایانش ابری، یک فراهم‌کننده به‌طور معمول به‌عنوان فراهم‌کننده خدمت ابری و کارفرما به‌عنوان مشتری خدمت ابری نامیده می‌شود. در برخی از موارد، فراهم‌کننده خدمت ابری مدیریت یا کنترل مؤلفه‌ها، منابع و فرایندها را به مشتری خدمت ابری واگذار می‌کند. این کار در محیطی انجام می‌شود که می‌تواند با دیگر مشتریان خدمت ابری مشترک باشد و به‌طور معمول به‌عنوان محیط ابری چند-مستأجر[1] شناخته می‌شود. ملاحظات امنیتی

1- Multi-tanent cloud environment

زنجیره تأمین ICT در زمانی که خدمات رایانش ابری تشکیل یک زنجیره تأمین ICT می‌دهند، مانند زمانی که یک مشتری از یک SaaS ساخته‌شده بر فراز IaaS استفاده می‌کند، نیز برقرار هستند.

۳-۵ مخاطرات امنیت اطلاعات در روابط تأمین‌کننده و تهدیدهای مرتبط با آن

مخاطرات امنیت اطلاعات در روابط تأمین‌کننده، نه تنها برای کارفرما و تأمین‌کننده، بلکه برای مشتریان و دیگر ذینفعان نیز یک موضوع نگرانی محسوب می‌شوند. این موردی از مسئله اعتماد در فعالیت‌های کسب‌وکاری در جامعه است. توصیه می‌شود، هر دو طرف تأمین‌کننده و کارفرما مخاطرات ذاتی و دیگر مخاطرات امنیت اطلاعات مرتبط با ایجاد یک رابطه تأمین‌کننده را در نظر بگیرند.

هر دو طرف تأمین‌کننده و کارفرما به یک اندازه در مورد قابل‌اعتماد ساختن توافق خود و مدیریت مخاطرات امنیت اطلاعات که شامل ایجاد نقش‌ها و مسئولیت‌های مشخص برای امنیت اطلاعات و پیاده‌سازی کنترل‌ها است، مسئولیت دارند.

هریک از روابط تأمین‌کننده در سازمان برای منظور خاصی ایجاد می‌شود. تعداد این روابط به احتمال به مرور زمان زیاد شده و این رشد، عدم مدیریت و کنترل صحیح روابط بیان‌شده توسط کارفرما را به همراه دارد. به‌ویژه، سازمان‌های بزرگ به‌طور معمول دارای تعداد چشمگیری از روابط تأمین‌کننده که به‌وسیله هستارهای داخلی مختلف با استفاده از فرایندها و آرایش‌های گوناگون ایجاد شده‌اند، هستند. بسیاری از این روابط دارای زنجیره تأمین گسترش‌یافته با چند لایه هستند. این چندگانگی می‌تواند حصول اطمینان از این‌که مخاطرات امنیت اطلاعات ایجادشده به‌وسیله روابط تأمین‌کننده بیان‌شده به شکل مناسب در نظر گرفته شده‌اند را به شکل فزاینده‌ای مشکل‌تر سازد.

تأمین و پشتیبانی یک محصول یا خدمت می‌تواند وابسته به انتقال اطلاعات یا سامانه اطلاعاتی از جانب کارفرما یا تأمین‌کننده به شخص دیگر باشد. لازم است که اطلاعات بیان‌شده به شکل مناسب از طریق ایجاد توافقی میان کارفرما و تأمین‌کننده حفظ شود. این توافق باید یک مجموعه از کنترل‌ها و مسئولیت‌های موردپذیرش اشخاص را برای پیاده‌سازی بیان کند. ممکن است عدم وجود چنین توافقی به روش‌های زیر بر روی امنیت اطلاعات کارفرما یا تأمین‌کننده تأثیرگذار باشد:

الف) عملکرد متفاوت کارفرما و تأمین‌کننده در زمینه راهبری امنیت اطلاعات، تحمل مخاطره و انطباق یا تفاوت‌های رفتار فرهنگی یا سازمانی که منجر به شکاف در الزامات امنیتی و کنترل‌ها میان کارفرما و تأمین‌کننده است.

ب) اتکا بر خدمات و قابلیت‌هایی از سوی تأمین‌کننده که برای اطمینان از مطابقت با الزامات امنیت اطلاعات خود کارفرما طراحی شده‌اند. این کار موجب وابستگی‌های غیرعمدی کنترل‌ها می‌شود.

پ) کنترل‌های امنیت اطلاعات متناقض یا متفاوت که موجب تداخل یا تضعیف امنیت اطلاعات شخص مقابل می‌شود.

ممکن است روابط تأمین‌کننده تعدادی مخاطره امنیت اطلاعات برای هر دو طرف کارفرما و تأمین‌کننده ایجاد نمایند. در ادامه نمونه‌هایی از این گونه مخاطرات که بهتر است در طول چرخه حیات یک رابطه تأمین‌کننده –از برنامه‌ریزی تا اتمام- لحاظ شوند بیان می‌شود.

الف) عدم وجود یا ضعف راهبری:

۱) کارفرمایان کنترل خود را بر روی چگونگی ذخیره، پردازش، انتقال، ایجاد، تغییر و تخریب اطلاعات از دست می‌دهند.

۲) ممکن است تأمین‌کنندگان بخشی از منابع و فرایندها را، مگر در حالتی که در توافق به‌طور مشخص منع شده باشند، به تأمین‌کننده دیگری برون‌سپاری نمایند. در نتیجه این اقدام کنترل کارفرما محدود شده و ممکن است کارفرما در معرض مخاطرات بعدی قرار گیرد.

ب) سوء ارتباط و سوءتفاهم:

۱) کنترل‌های فراهم‌شده از سوی تأمین‌کننده مخاطرات شناسایی‌شده توسط کارفرما را پوشش نمی‌دهند و در نتیجه کارفرما در برابر مخاطراتی که تصور می‌شود تأمین‌کننده کنترل کرده است آسیب‌پذیر باقی می‌ماند.

۲) ممکن است الزامات محرمانگی[1]، یکپارچگی[2] و دسترس‌پذیری کارفرما به شکل صحیح به تأمین‌کننده منتقل نشده و درنتیجه رعایت نشوند.

۳) الزامات مربوط به دسترس‌پذیری/BCP برای اطلاعات یا سامانه‌های اطلاعاتی که تحویل به‌موقع محصولات و خدمات از جانب تأمین‌کننده را پشتیبانی می‌کنند، نمی‌توانند مشخص شوند و این موجب اختلال در تأمین می‌شود.

۴) تأمین‌کننده در تخصیص منابع کافی شامل نیروی متخصص برای محافظت از اطلاعات کارفرما موفق عمل نمی‌کند.

پ) تفاوت‌های جغرافیایی، اجتماعی و فرهنگی.

۱) کارفرما به‌صورت غیرعمدی در نقض قوانین یا مقررات مشارکت می‌کند که منجر به آسیب به شهرت و جریمه‌های مالی می‌شود.

۲) ارجاع به یک قانون[3] یا یک استاندارد به‌عنوان یک الزام در یک توافقنامه امکان سوء تفسیر توسط کارفرما

1- Confidentiality
2- Integrity
3- Law

و تأمین‌کننده را فراهم می‌کند که این موجب اختلاف می‌شود.

۳) خدمت موردنظر در مکانی نامشخص یا غیرمجاز از نظر کارفرما فراهم شده است که موجب نقض الزامات قانونی[1] یا توافقی کارفرما شده است.

مخاطرات خاصی در مورد اطلاعات و سامانه‌های اطلاعاتی کارفرما و تأمین‌کننده می‌توانند به‌طور مستقیم با آگاهی از کنترل ، مالکیت و پاسخگویی ناکافی مرتبط شوند. ممکن است، این مخاطرات در هر دو مورد محصولات و خدمات صادق باشند. جدول ۱ نمونه‌هایی از مخاطرات امنیت اطلاعات مربوط به اکتساب محصولات را فراهم می‌کند. مخاطرات امنیت اطلاعات مربوط به خدمات به‌طور معمول به دلیل دسترسی تأمین‌کننده به اطلاعات یا سامانه‌های اطلاعاتی ایجاد می‌شوند. جدول ۲ نمونه‌هایی از مخاطرات مربوط به دسترسی تأمین‌کننده به اطلاعات و سامانه‌های اطلاعاتی را فراهم می‌کند.

جدول ۱ ــ مخاطرات نمونه امنیت اطلاعات برای اکتساب محصولات

شماره	نوع	توضیحات
۱	ویژگی امنیت اطلاعات	در موردی که یک محصول تأمین‌شده دارای آسیب‌پذیری باشد، محصولاتی که کارفرما بر مبنای آن‌ها تولید می‌کند نیز آسیب‌پذیر خواهند بود.
۲	کیفیت	کیفیت پایین محصولات تأمین‌شده می‌تواند موجب ضعف محصولات، خدمات و فرایندهای مشتق‌شده کارفرما باشد.
۳	مالکیت معنوی	دارایی معنوی شناسایی‌نشده می‌تواند موجب اختلاف در ارتباط به خدمات و محصولات مشتق‌شده کارفرما شود.
۴	اصالت	در موردی که محصولات جعلی یا تقلبی تأمین شده باشند، انتظار کارفرما از یک ویژگی امنیت اطلاعات و کیفیت و شناسایی مالکیت معنوی با احتمال معرفی یک ضعف امنیت اطلاعات و از دست دادن اعتماد رابطه کسب‌وکاری تهدید می‌شود.
۵	تضمین	بدون تضمین ویژگی‌های امنیت اطلاعات مناسب کیفیت محصول و شناسایی مالکیت معنوی و اصالت کارفرما اعتماد خود را به محصولات تأمین‌کننده از دست می‌دهد.

جدول ۲ ــ مخاطرات نمونه امنیت اطلاعات برای اکتساب خدمات

شماره	نوع	توضیحات	مورد(موارد) کاربرد نمونه
۱	دسترسی فیزیکی در محل	تأمین‌کننده به تسهیلات پردازش اطلاعات کارفرما دسترسی داشته اما دسترسی منطقی ندارد.	خدمت محافظ امنیتی، خدمات تحویل، یک خدمت پاک‌سازی یا یک خدمت نگهداشت تجهیزات
۲	دسترسی به اطلاعات و سامانه‌های	کارکنان تأمین‌کننده در محل بوده و از طریق تجهیزات کارفرما به اطلاعات و سامانه‌های اطلاعاتی	متخصص مربوط به موارد برون‌سپاری‌شده که در محل کار کرده و با تیم کارفرما یکپارچه

1- Regulatory

	اطلاعاتی در محل	دسترسی منطقی دارند.	شده است.
۳	دسترسی از راه دور به اطلاعات و سامانه‌های اطلاعاتی داخلی	تأمین‌کننده به اطلاعات و سامانه‌های کارفرما دسترسی از راه دور دارد.	فعالیت‌های توسعه و نگهداشت از راه دور، مدیریت سامانه‌های اطلاعاتی و تجهیزات از راه دور، آماد، عملیات مرکز تماس، سامانه‌های مدیریت تسهیلات خودکار
۴	پردازش اطلاعات در خارج از محل	اطلاعات تحت مسئولیت کارفرما توسط تأمین‌کننده در خارج از محل به‌وسیله برنامه‌های کاربردی و سامانه‌های تحت کنترل و مدیریت تأمین‌کننده پردازش می‌شوند.	مشاوره(تحقیق بازار، تبلیغات فروش، مطالعات فنی و غیره). تأمین‌کنندگان پردازش اطلاعات، R&D، تولید، ذخیره‌سازی و بایگانی، خدمت برنامه کاربردی (ASP)، فرایند کسب‌وکار به‌عنوان یک خدمت(BPaaS) مانند خدمات مسافرتی یا مالی،زیرساخت به‌عنوان یک خدمت(IaaS) یا نرم‌افزار به‌عنوان یک خدمت (SaaS)
۵	برنامه کاربردی در خارج از محل	برنامه‌هایی که توسط کارفرما استفاده می‌شوند PaaS یا IaaS اجرا می‌کنند.	فراهم‌کنندگان سکو به‌عنوان یک خدمت (PaaS) در صورتی که تأمین‌کننده سکوهای توسعه را فراهم کند یا فراهم‌کنندگان IaaS اگر تأمین‌کننده خدمات شبکه، رایانش و ذخیره‌سازی را فراهم آورد.
۶	تجهیزات در خارج از محل	تجهیزات اختصاص‌یافته به کارفرما و تحت مالکیت در خارج از محل، در محل تأمین‌کننده میزبانی می‌شوند.	میزبانی سامانه‌های اطلاعاتی در خارج از محل یا IaaS
۷	ذخیره اطلاعات در خارج از محل	کارفرما ذخیره اطلاعات را برای نگهداری یا بایگانی در خارج از محل به یک تأمین‌کننده برون‌سپاری می‌کند.	استفاده از خدمت ذخیره‌سازی برای نگهداشت رونوشت‌های پشتیبان از اطلاعات که به‌وسیله پردازش اطلاعات به‌صورت داخلی ایجاد شده‌اند

۸	امان‌سپاری[1] کد منبع	خدماتی که شامل فراورده‌هایی از تأمین‌کننده هستند که توسط کارفرما استفاده می‌شوند، به‌صورت امان‌سپاری نزد شخص سوم مطمئن نگهداری شده و تحت شرایط تعریف‌شده در دسترس کارفرما قرار می‌گیرند.	کد منبع نگهداری شده به‌وسیله شخص سوم مستقل برای نگهداشت قابلیت استفاده نرم‌افزار توسط کارفرما در شرایطی که تأمین‌کننده نرم‌افزار کسب‌وکار خود را ترک می‌کند.

۴-۵ مدیریت مخاطرات امنیت اطلاعات در روابط تأمین‌کننده

در رابطه تأمین‌کننده، دسترسی کارفرما یا تأمین‌کننده به اطلاعات سازمان دیگر و اداره آن می‌تواند برای هر دو طرف کارفرما و تأمین‌کننده مخاطره امنیتی ایجاد کند. کارفرما و تأمین‌کننده مخاطرات را ارزیابی کرده و کنترل‌هایی را به‌منظور کاهش آن‌ها انتخاب و پیاده‌سازی می‌کنند. در زمینه روابط تأمین‌کننده، کنترل از موارد زیر تشکیل می‌شود:

الف) آن‌هایی که به‌طور مستقیم مخاطرات امنیت اطلاعات مربوط به دسترسی یا اداره هر یک از اقلام اطلاعاتی سازمان را پوشش می‌دهند.

ب) آن‌هایی که کیفیت آن دسته از محصولات تأمین‌کننده را که بر روی مخاطرات امنیت اطلاعات تأمین‌کننده و مشتریان آن تأثیرگذار است پوشش می‌دهد.

پ) آن‌هایی که موارد الف و ب بالا را بر روی سازمان دیگر با روش‌هایی مانند مدیریت و گزارش الزامات، پایش، ممیزی و مجوزدهی اعمال می‌کنند.

توافقنامه میان کارفرما و تأمین‌کننده، هر دو سازمان را به پیاده‌سازی و نگهداشت کنترل‌های بیان‌شده مقید می‌کند.

فارغ از ماهیت محصول یا خدمت تأمین‌شده، مشاهده‌پذیری امنیت اطلاعات باید به‌عنوان قسمت مهمی از ایجاد رابطه تأمین‌کننده به‌منظور اطمینان از مدیریت شدن مخاطرات اطلاعات و سامانه‌های اطلاعاتی کارفرما مورد توجه قرار گیرد. به‌منظور شناسایی و مدیریت این مخاطرات امنیت اطلاعات، کارفرما باید اطمینان حاصل کند که تأمین‌کننده کنترل‌ها و مدیریت کافی را در زمینه امنیت اطلاعات پیاده‌سازی کرده است. در صورتی که این موارد قابل مذاکره نباشند، توصیه می‌شود کارفرما یک خدمت یا محصول تأمین‌کننده را بر مبنای معیارهایی که شامل الزامات مدیریت و کنترل‌های امنیت اطلاعات به‌منظور اجتناب یا کاهش مخاطرات به یک سطح قابل قبول هستند، انتخاب کند.

1- Escrow

۵-۵ ملاحظات زنجیره تأمین ICT

پذیرش تولید، تحویل و عملیاتی شدن محصولات توسط تأمین‌کننده باید بر مبنای معیارهایی انجام شود که سطوح امنیت اطلاعات مدنظر کارفرما در داخل سازمان خود را تضمین کند. این معیارها می‌توانند شامل هر یک از موارد زیر باشند:

- مدیریت مخاطرات سیاسی، قانونی[1] و امنیت اطلاعات مربوط به محیط محلی که بر روی امنیت اطلاعات کارفرما شامل تداوم اطلاعات، سامانه‌های اطلاعاتی و خدمات تأثیرگذار است.

- مدیریت محرمانگی مستندات الکترونیکی و فیزیکی و دیگر اطلاعات مرتبط با محصولات و خدمات تأمین‌شده.

- مدیریت یکپارچگی موارد و مؤلفه‌ها برای اطمینان از اداره مناسب آن‌ها مانند نشانه‌گذاری و برچسب‌گذاری حفاظتی یکسان

- مدیریت یکپارچگی نرم‌افزار یا دیگر اطلاعات الکترونیکی مربوط به محصول یا خدمت تأمین‌شده برای اطمینان از آن‌که دچار مشکلی نشده باشد؛ به‌عنوان‌مثال تابع چکیده‌ساز رمزنگاشتی[2] یا نشان‌گذاری رقمی[3] می‌توانند استفاده شوند.

- مدیریت امنیت فیزیکی تسهیلاتی که از محصولات و خدمات از آن‌ها تحویل شده‌اند.

- مدیریت امنیت اطلاعات مربوط به هر یک از جنبه‌های کسب‌وکار تأمین‌کننده و هر یک از کارخواه‌های[4] دیگر.

- مدیریت امنیت اطلاعات مربوط به هر یک از جنبه‌های کسب‌وکار تأمین‌کننده، تعاملات تأمین‌کننده با تأمین‌کنندگان خود و روابط تأمین‌کننده با دیگر کارفرمایان.

به‌منظور مدیریت مناسب امنیت اطلاعات در روابط تأمین‌کننده در سراسر زنجیره تأمین ICT، کارفرمایان باید چارچوبی از فرآیندهای استاندارد در سطح سازمان را برای اکتساب محصولات و خدمات مورد پذیرش با مجموعه زیر قرار دهند:

الف) الزامات امنیت اطلاعات و انطباق برای تبادل یا اشتراک امن اطلاعات و سامانه‌های اطلاعاتی ایجاد شود.

ب) مخاطرات امنیتی مربوط به زنجیره تأمین پیش از اکتساب ارزیابی و پایش شوند.

1- Legal
2- Cryptographic hash function
3- Digital watermark
4- Clients

پ) فرایندی برای مذاکره یا مذاکره مجدد توافق یا توافق‌های زنجیره تأمین ICT شامل الزامات امنیت اطلاعات و انطباق شامل شرایطی برای حق ممیزی و محدود کردن تأمین‌کنندگان بالادست از طریق چندین لایه زنجیره تأمین ICT ایجاد شود.

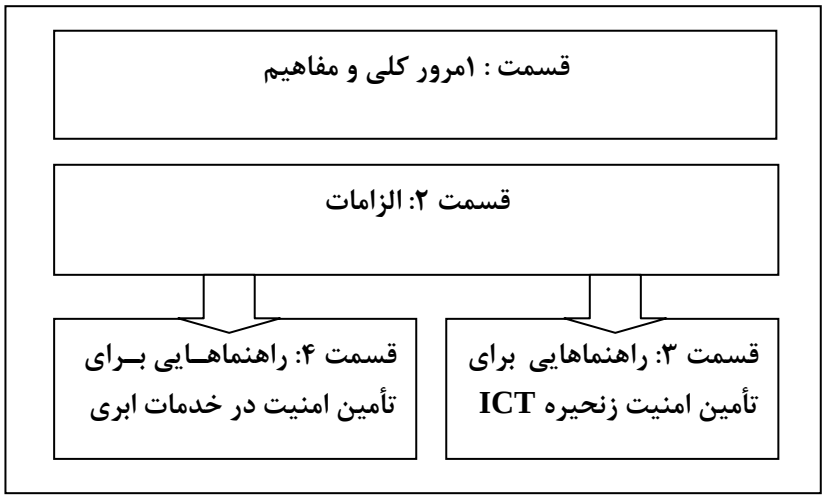
ت) کارایی تأمین‌کنندگان زنجیره تأمین ICT را با توجه به الزامات امنیت اطلاعات و انطباق به‌ویژه در نتیجه تغییرات در رابطه تأمین‌کننده، به‌صورت مستمر پایش و گزارش شود.

این چارچوب باید به‌منظور پوشش محدوده‌ای از توافقات ICT که ممکن است مناسب طبیعت محصول یا خدمت اکتساب‌شده و مخاطراتی که انتظار می‌رود ایجاد کند متناسب‌سازی شوند، انعطاف‌پذیر باشد.

۶ ساختار کلی ISO/IEC 27036 و مرور کلی

۶-۱ هدف و ساختار

ISO/IEC 27036 یک استاندارد چندقسمتی است که در زمینه چگونگی ایمن‌سازی اطلاعات در رابطه تأمین‌کننده برای کارفرما و تأمین‌کننده، الزامات و راهنمایی فراهم می‌کند. شکل ۲ معماری این استاندارد بین‌المللی چندقسمتی را نمایش می‌دهد.



شکل ۲- معماری ISO/IEC 27036

قسمت ۳ و ۴ جنبه‌های خاص امنیت اطلاعات روابط تأمین‌کننده شامل چالش‌های مربوط به جنبه‌های مرتبط به خدمات و محصولات ICT (قسمت ۳) و خدمات ابری (قسمت ۴) را نمایش می‌دهد.

۶-۲ مرور کلی قسمت ۱: مرور کلی و مفاهیم

قسمت ۱ (مستند حاضر) مرور کلی و مفاهیم امنیت اطلاعات در روابط تأمین‌کننده را فراهم می‌کند. قسمت ۱ یک مستند اطلاعاتی است.

۶-۳ مرور کلی قسمت ۲: الزامات

قسمت ۲ یک چارچوب سطح بالا برای ایجاد الزامات و انتظارات امنیت اطلاعات در روابط تأمین‌کننده فراهم می‌کند. این چارچوب شامل راهبری، فرایندهای چرخه حیات چارچوب و بیانیه‌های الزامات سطح بالای مرتبط است. قسمت ۲ یک استاندارد الزامی است که کارفرمایان می‌توانند به‌عنوان مرجع الزامات توافقنامه برای تعریف مدیریت و پایش توافق تأمین‌کننده از آن استفاده نمایند. ممکن است الزامات این استاندارد به‌عنوان معیارهای تکمیلی مجوزدهی در راستای اهداف مجوزدهی ISO/IEC 27001 کارفرمایی الزام کند که تأمین‌کننده دارای گواهی مربوط به ISO/IEC 27001 بوده و الزامات تکمیلی و کنترل‌های قابل‌اعمال در ارتباط با ISO/IEC 27036 را یا توجه به محصولات یا خدمات ارائه‌شده نیز رعایت کند. ممکن است کارفرمایان از کل استاندارد استفاده کرده و بخش‌های منفردی را برای استفاده به‌عنوان بیانیه الزامات استخراج نمایند.

۶-۴ مرور کلی قسمت ۳: راهنماهایی برای امنیت زنجیره تأمین فناوری اطلاعات و ارتباطات(ICT) در روابط تأمین‌کننده

- در روابط تأمین‌کننده یک محصول یا خدمت ICT که توسط کارفرما، کسب می‌شود لزوماً تنها توسط یک تأمین‌کننده تولید یا عملیاتی نمی‌شود. به‌عنوان‌مثال یک محصول به‌طورمعمول شامل قسمت‌هایی است که توسط تأمین‌کنندگان دیگر ساخته شده و به‌عنوان روابط غیرمستقیم با کارفرما، برای تأمین‌کننده فراهم شده‌اند. یا یک خدمت پردازش اطلاعات می‌تواند از خدمات پردازش اطلاعات دیگر به‌عنوان زیرساخت اولیه استفاده کند. به‌عنوان نمونه، یک تأمین‌کننده می‌تواند با تأمین‌کننده دیگری برای نگهداشت سخت‌افزار، ذخیره نسخه‌های پشتیبان بر روی یک محل خارجی، یا حتی برون‌سپاری کل فرایند پشتیبان‌گیری توافقنامه داشته باشد. بنابراین، زنجیره‌های تأمین فناوری اطلاعات به‌وسیله سلسله روابط تأمین‌کننده با وابستگی‌های متقابل ذاتی شکل می‌گیرند.

در یک زنجیره تأمین، مدیریت وکنترل‌های امنیت اطلاعات پیاده‌سازی‌شده توسط تأمین‌کننده در ارتباط مستقیم با کارفرما همیشه برای مدیریت مخاطرات امنیت اطلاعات یک محصول یا خدمت کافی نیستند. مدیریت تأمین‌کنندگان غیرمستقیم(تأمین‌کننده‌ی تأمین‌کننده) محصول یا خدمت می‌تواند برای امنیت اطلاعات لازم باشد: این کار نیازمند مشاهده‌پذیری در زنجیره تأمین است.

از طرف دیگر، تأمین‌کنندگان نیز می‌توانند مخاطرات فزاینده امنیت اطلاعات ایجادشده به دلیل اتصال متقابل سامانه‌های کارفرما و تأمین‌کننده را که گاهی اوقات در نتیجه زنجیره تأمین ICT ایجاد می‌شود تجربه نمایند. برای مثال، کارفرما می‌تواند ممیزی‌های مهاجمی را الزامی کند که می‌توانند منجر به دسترسی کارفرما به دارایی‌های معنوی تأمین‌کننده شوند.

قسمت ۳ استاندارد ISO/IEC 27036 راهنماهایی برای کارفرمایان و تأمین‌کنندگان برای مدیریت مخاطرات امنیت اطلاعات مربوطبه زنجیره تأمین محصولات و خدمات ICT فراهم می‌کند. این قسمت بر

روی الزامات قسمت ۲ ساخته شده و اعمال تکمیلی برای تقویت الزامات سطح بالای قسمت ۲ فراهم می‌کند.

۶-۵ مرور کلی قسمت ۴: راهنماهایی برای امنیت خدمات ابری

سازمان‌ها، از خدمات رایانش ابری برای بهره‌مند شدن از صرفه‌جویی‌های مقیاس فراهم‌شده توسط رایانش ارتجاعی و قابلیت‌های خدمت ذخیره‌سازی استفاده می‌کنند. این قابلیت‌ها در قالب یک مدل مبتنی بر کاربرد یا برمبنای استفاده در دسترس قرار می‌گیرند. رایانش ابری می‌تواند در چند مدل متفاوت ارائه خدمت ابری مانند IaaS، PaaS و SaaS فراهم شود. با این وجود، این کار مخاطرات امنیت اطلاعات مربوط به اتصال متقابل پیچیده بزرگ‌تر کارفرما و تأمین‌کننده را به همراه دارد. مانند مخاطرات امنیت اطلاعات زنجیره تأمین ICT، امکان کمبود شفافیت در نقش‌ها و مسئولیت‌های مدیریت امنیت اطلاعات و پیاده‌سازی کنترل‌ها وجود دارد.

برای مثال، اگر بارهای کاری خدمت رایانش ابری مرزهای ملی را رد کند یا مشتری رایانش ابری قادر به کنترل چگونگی تحویل خدمت ابری نباشد، ممکن است به مخاطرات نقض قانونی[1] تعهدات توافق توسط کارفرما یا تأمین‌کننده منجر شود. علاوه بر آن، مالکیت چندگانه و استفاده از فناوری‌ها (مانند مجازی‌سازی و واسط‌های برنامه کاربردی (API)) می‌تواند منجر به مخاطرات امنیت اطلاعات زیادی برای محرمانگی مشتری ابری به‌عنوان عواقب کنترل دسترسی ناکافی و کمبود تفکیک مشتری خدمت ابری شود.

قسمت ۴ استاندارد ISO/IEC 27036 راهنماهایی برای امنیت اطلاعات خدمات رایانش ابری را که به‌طور معمول از طریق زنجیره تأمین فراهم می‌شوند از دیدگاه هر دو طرف کارفرما و تأمین‌کننده خدمات بیان‌شده ارائه می‌دهد. به‌طور مشخص این استاندارد مدیریت مخاطرات امنیت اطلاعات مربوط‌به خدمات رایانش ابری در سراسر چرخه حیات رابطه تأمین‌کننده را در بر می‌گیرد. این قسمت از استاندارد بر روی الزامات قسمت دوم ساخته شده و اعمال تکمیلی برای تقویت الزامات سطح بالای قسمت ۲ و راهنماهای قسمت ۳ را فراهم می‌کند.

1- Legal

کتاب‌نامه

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

[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 ۲۷۰۰۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت مخاطرات امنیت اطلاعات

[۴] استاندارد ملی ایران شماره ۲۷۰۱۴: سال ۱۳۹۱، فناوری اطلاعات - فنون امنیتی - حاکمیت امنیت اطلاعات

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

[۶] استاندارد ملی ایران شماره ۲۸۰۰۰ : سال ۱۳۸۷، سامانه‌های مدیریت امنیت زنجیره تأمین مشخصات

[۷] استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷، سامانه‌های مدیریت کیفیت - مبانی و واژگان

[۸] استاندارد ملی ایران شماره ۱۶۰۳۴: سال ۱۳۹۱، مهندسی سامانه‌ها و نرم افزار- فرایندهای چرخه حیات سامانه

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

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