Learn Today,

Activate Tomorrow

ترجمه استاندارد

ISO/IEC 27001:2013

Information Security Management Systems

فهرست مطالب

مقدمه

امروزه امنیت اطلاعات یکی از چالش‌های اصلی در عصر فناوری اطلاعات محسوب می‌شود و حفاظت از اطلاعات در برابر دسترسی غیرمجاز، تغییرات، خرابکاری و افشا، امری ضروری و اجتناب ناپذیر به شمار می‌رود. از اینرو، امنیت دارایی‌های اطلاعاتی، برای تمامی سازمان‌ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش است. فراهم‌آوری صحت و تمامیت اطلاعات، به گونه‌ای که در زمان مناسب، اطلاعات در دسترس افراد مجازی قرار گیرد که نیازمند آن هستند، عاملی است که منجر به اثربخشی کسب و کار می‌گردد. این مسئله در سال‌های اخیر، با افزایش تهدیدات و حملات سایبری به سازمان‌ها و روند رو به گسترش آن، مورد توجه جدی مسئولین و کارشناسان مربوطه قرار گرفته است.

از سوی دیگر، در دو دهه اخیر با ایجاد نگرش استانداردی به امنیت اطلاعات، استانداردهای مفیدی در این حوزه تدوین شده است. استاندارد ISO/IEC 27001 که مهمترین و پرمراجعه‌ترین استاندارد در این خصوص است، زمینه مناسبی را برای طراحی و استقرار سیستم مدیریت امنیت اطلاعات و ارزیابی آن در سازمان‌ها و همچنین بهره‌گیری از منافع این رویکرد فراهم آورده است.

کتاب حاضر، ترجمه استاندارد ISO/IEC 27001 ویرایش ۲۰۱۳ است که در راستای نگاه سیستمی به امنیت اطلاعات در کشورمان، تهیه شده و به صورت رایگان، در اختیار علاقه‌مندان قرار گرفته است. در انتهای این کتاب نیز نسخه اصلی استاندارد، جهت استفاده کارشناسان آورده شده است.

آکادمی باتیس
خرداد ۱۳۹۳

پیشگفتار

سازمان بین‌المللی استاندارد (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC)، سیستمی تخصصی را جهت استانداردسازی در سطح دنیا ایجاد نموده‌اند. نهادهای ملی عضو ISO یا IEC، توسط کمیته‌های فنی تدوین شده از سوی سازمان مربوطه‌شان، در تدوین استانداردهای بین‌المللی مشارکت می‌کنند و به زمینه‌های خاص فعالیت‌های فنی می‌پردازند. کمیته‌های فنی ISO و IEC، در زمینه‌هایی با منافع مشترک، با همدیگر همکاری می‌کنند. سایر سازمان‌های بین‌المللی، دولتی یا غیردولتی وابسته به ISO و IEC نیز در این زمینه مشارکت دارند. ISO و IEC، کمیته فنی مشترکی را در حوزه فناوری اطلاعات تحت عنوان ISO/IEC JTC 1 تشکیل داده‌اند.

پیش‌نویس استانداردهای بین‌المللی، مطابق با قوانین مندرج در بخش ۲ دستورالعمل‌های ISO/IEC تهیه شده است.

وظیفه اصلی کمیته فنی مشترک، آماده‌سازی استانداردهای بین‌المللی است. پیش‌نویس استانداردهای بین‌المللی مورد تأیید کمیته فنی مشترک، برای رأی‌گیری در اختیار نهادهای ملی قرار می‌گیرد. انتشار به عنوان استاندارد بین‌المللی منوط به تأیید حداقل ۷۵٪ نهادهای ملی رأی دهنده است.

به این احتمال که ممکن است برخی عناصر این سند، تحت حقوق ثبت اختراع باشند هم توجه شده است. ISO و IEC مسئولیتی در قبال شناسایی هر یک یا همه این حقوق ندارند.

ISO/IEC 27001 توسط کمیته فرعی SC 27، فنون امنیتی فناوری اطلاعات، زیرمجموعه کمیته فنی مشترک ISO/IEC JTC 1، فناوری اطلاعات، تهیه شده است.

این ویرایش دوم، جایگزین و باطل کننده ویرایش اول (ISO/IEC 27001:2005) است که از نظر فنی مورد بازنگری قرار گرفته است.

۰. مقدمه

۱،۰ کلیات

این استاندارد بین‌المللی، به منظور ارایه الزاماتی برای استقرار، پیاده‌سازی، نگهداری و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات تهیه شده است. پذیرش یک سیستم مدیریت امنیت اطلاعات، یک تصمیم استراتژیک برای یک سازمان است. استقرار و پیاده‌سازی سیستم مدیریت امنیت اطلاعات در یک سازمان، تحت تأثیر نیازها و اهداف سازمان، الزامات امنیتی، فرایندهای سازمانی به کار گرفته شده و اندازه و ساختار سازمان قرار دارد. انتظار می‌رود تمامی این عوامل اثرگذار، در طول زمان دچار تغییر شوند.

سیستم مدیریت امنیت اطلاعات، با به کارگیری یک فرایند مدیریت مخاطرات، از محرمانگی، صحت و دسترس‌پذیری اطلاعات محافظت می‌کند و به طرف‌های ذینفع این اطمینان را می‌دهد که مخاطرات، به میزان کافی مدیریت می‌شوند.

توجه داشته باشید که سیستم مدیریت امنیت اطلاعات، با فرایندهای سازمان و ساختار مدیریتی کلان، یکپارچه بوده و بخشی از آنها است و همچنین امنیت اطلاعات در طراحی، فرایندها، سیستم‌های اطلاعاتی و کنترل‌ها لحاظ می‌شود. انتظار می‌رود که پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات، منطبق با نیازهای سازمان باشد.

این استاندارد بین‌المللی می‌تواند توسط طرف‌های درونی و بیرونی، به منظور ارزیابی توانایی یک سازمان در فراهم‌آوری الزامات امنیت اطلاعات خود، مورد استفاده قرار گیرد.

ترتیب ارایه الزامات در این استاندارد بین‌المللی، بیان کننده اهمیت یا ترتیب پیاده‌سازی آنها نیست. موارد فهرست شده، به منظور ارجاع‌های بعدی ذکر شده شداند.

استاندارد ISO/IEC 27000، نمای کلی و واژگان سیستم‌های مدیریت امنیت اطلاعات را توصیف نموده و مرجع خانواده استاندارد سیستم مدیریت امنیت اطلاعات (شامل ISO/IEC 27003[۲]، ISO/IEC 27004[۳] و ISO/IEC 27005[۴]) به همراه اصطلاحات و تعاریف مرتبط با آن است.

۲,۰ سازگاری با سایر استانداردهای سیستم مدیریت

این استاندارد بین‌المللی از ساختار سطح بالا، عناوین یکسان در بندهای فرعی، متن یکسان، اصطلاحات مشترک و تعاریف اصلی موجود در پیوست SL بخش ۱ دستورالعمل‌های ISO/IEC، مکمل‌های تلفیقی ISO استفاده می‌کند و در نتیجه با سایر استانداردهای سیستم مدیریت که پیوست SL را پذیرفته‌اند، سازگار است.

این رویکرد مشترک که در پیوست SL تعریف شده است، برای آن دسته از سازمان‌هایی که درنظر دارند یک سیستم مدیریت واحد را در راستای فراهم‌آوری الزامات دو یا چند استاندارد سیستم مدیریت اجرا کنند، مفید خواهد بود.

فناوری اطلاعات – فنون امنیتی – سیستم‌های مدیریت امنیت اطلاعات – الزامات

۱. قلمرو

این استاندارد بین‌المللی، الزاماتی را برای استقرار، پیاده‌سازی، نگهداری و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات در چارچوب سازمان، مشخص می‌کند. این استاندارد بین‌المللی، همچنین شامل الزاماتی برای ارزیابی و برطرف‌سازی مخاطرات امنیت اطلاعات، متناسب با نیازهای سازمان است. الزامات تعیین شده در این استاندارد بین‌المللی، عمومی بوده و در تمام سازمان‌ها، صرف‌نظر از نوع، اندازه یا ماهیت آنها، قابل اعمال است. کنارگذاری هر یک از الزامات مشخص شده در بندهای ۴ تا ۱۰، چنانچه یک سازمان ادعای تطابق با این استاندارد بین‌المللی را داشته باشد، مورد پذیرش نخواهد بود.

۲. مراجع اصلی

اسناد زیر، به صورت کلی و جزئی، در این سند به صورت الزامی، مورد ارجاع قرار گرفته‌اند و در راستای کاربرد این سند، مراجعی که با ذکر تاریخ، ارجاع داده شده‌اند فقط همان ویرایش، و مراجعی که بدون ذکر تاریخ، ارجاع داده شده‌اند آخرین ویرایش سند اشاره شده (شامل همه اصلاحیه‌ها) مورد استناد است.

ISO/IEC 27000، فناوری اطلاعات – فنون امنیتی – سیستم‌های مدیریت امنیت اطلاعات – نمای کلی و واژگان

۳. اصطلاحات و تعاریف

در راستای اهداف این سند، اصطلاحات و تعاریف ذکر شده در ISO/IEC 27000 به کار می‌روند.

۴. چارچوب سازمان

۱,۴ شناخت سازمان و چارچوب آن

سازمان باید مسایل درونی و بیرونی مرتبط با اهداف سازمان و مسایل تأثیرگذار در امکان دستیابی به نتایج مورد نظر سیستم مدیریت امنیت اطلاعات را شناسایی کند.

نکته: تعیین این مسایل به استقرار چارچوب بیرونی و درونی سازمان که در بند ۳,۵ از استاندارد ISO 31000:2009[۵] مطرح شده است، اشاره دارد.

۲,۴ شناخت نیازها و انتظارات طرف‌های ذینفع

سازمان باید موارد زیر را مشخص کند:

الف) طرف‌های ذینفع مرتبط با سیستم مدیریت امنیت اطلاعات؛ و

ب) الزامات این طرف‌های ذینفع در ارتباط با امنیت اطلاعات.

نکته: الزامات طرف‌های ذینفع، ممکن است شامل الزامات قانونی، مقرراتی و تعهدات قراردادی باشد.

۳,۴ تعیین قلمرو سیستم مدیریت امنیت اطلاعات

سازمان باید مرزها و کاربردپذیری سیستم مدیریت امنیت اطلاعات را به منظور استقرار قلمرو خود، شناسایی کند.

سازمان باید هنگام تعیین قلمرو، موارد زیر را درنظر بگیرد:

الف) مسایل بیرونی و درونی اشاره شده در بند ۱,۴؛

ب) الزامات اشاره شده در بند ۲,۴؛ و

ج) واسط‌ها و وابستگی‌های بین فعالیت‌های انجام شده توسط سازمان و فعالیت‌هایی که توسط سازمان‌های دیگر انجام می‌شوند.

قلمرو باید به صورت اطلاعات مستند، در دسترس باشد.

۴,۴ سیستم مدیریت امنیت اطلاعات

سازمان باید یک سیستم مدیریت امنیت اطلاعات را مطابق با الزامات این استاندارد بین‌المللی، ایجاد، پیاده‌سازی و نگهداری کند و آن را به طور مستمر بهبود بخشد.

۵. رهبری

۱,۵ رهبری و تعهد

مدیریت ارشد باید رهبری و تعهد خود را نسبت به سیستم مدیریت امنیت اطلاعات، از طریق موارد زیر نشان دهد:

الف) حصول اطمینان از اینکه خط‌مشی امنیت اطلاعات و اهداف امنیت اطلاعات، ایجاد شده و با مسیر استراتژیک سازمان سازگار هستند.

ب) حصول اطمینان از اینکه الزامات سیستم مدیریت امنیت اطلاعات در فرایندهای سازمان گنجانده شده‌اند.

ج) حصول اطمینان از اینکه منابع مورد نیاز سیستم مدیریت امنیت اطلاعات، در دسترس هستند.

د) ابلاغ اهمیت مدیریت امنیت اطلاعات اثربخش و تطابق با الزامات سیستم مدیریت امنیت اطلاعات؛

ه) اطمینان از اینکه سیستم مدیریت امنیت اطلاعات به نتیجه (نتایج) مورد انتظار دست می‌یابد.

و) هدایت و پشتیبانی از افراد برای کمک به اثربخشی سیستم مدیریت امنیت اطلاعات؛

ز) ترویج بهبود مستمر؛ و

ح) پشتیبانی از سایر نقش‌های مدیریتی مرتبط جهت نشان دادن رهبری آنها، به نحوی که در محدوده‌های مسئولیتی آنها اعمال گردد.

۲,۵ خط‌مشی

مدیریت ارشد باید یک خط‌مشی امنیت اطلاعات ایجاد کند که:

الف) متناسب با هدف سازمان باشد.

ب) شامل اهداف امنیت اطلاعات باشد (به بند ۲,۶ مراجعه شود) یا چارچوبی را برای تعیین اهداف امنیت اطلاعات ارایه دهد.

ج) شامل تعهدی مبنی بر فراهم‌آوری الزامات کاربردپذیر مرتبط با امنیت اطلاعات باشد؛ و

د) شامل تعهدی مبنی بر بهبود مستمر سیستم مدیریت امنیت اطلاعات باشد.

خط‌مشی امنیت اطلاعات باید:

ه) به صورت اطلاعات مستند، در دسترس باشد.

و) در داخل سازمان ابلاغ شود؛ و

ز) در صورت نیاز، در اختیار طرف‌های ذینفع قرار گیرد.

۳,۵ نقش‌های سازمانی، مسئولیت‌ها و اختیارات

مدیریت ارشد باید اطمینان حاصل کند که مسئولیت‌ها و اختیارات برای نقش‌های مرتبط با امنیت اطلاعات، تعیین و ابلاغ شده‌اند.

مدیریت ارشد باید مسئولیت و اختیارات را برای موارد زیر تعیین کند:

الف) حصول اطمینان از انطباق سیستم مدیریت امنیت اطلاعات با الزامات این استاندارد بین‌المللی؛ و

ب) گزارش عملکرد سیستم مدیریت امنیت اطلاعات به مدیریت ارشد.

نکته: مدیریت ارشد ممکن است مسئولیت‌ها و اختیاراتی را نیز برای گزارش عملکرد سیستم مدیریت امنیت اطلاعات در درون سازمان تعیین کند.

۶. طرح‌ریزی

۱,۶ اقداماتی برای درنظر گرفتن مخاطرات و فرصت‌ها

۱,۱,۶ کلیات

هنگام طراحی سیستم مدیریت امنیت اطلاعات، سازمان باید مسایل اشاره شده در بند ۱,۴ و الزامات اشاره شده در بند ۲,۴ را مدنظر قرار داده و مخاطرات و فرصت‌هایی را که نیازمند مقابله هستند، در راستای موارد زیر تعیین کند:

الف) حصول اطمینان از اینکه سیستم مدیریت امنیت اطلاعات می‌تواند به نتیجه (نتایج) مطلوب خود دست یابد.

ب) از بروز اثرات ناخواسته ممانعت نموده یا آنها را کاهش دهد؛ و

ج) به بهبود مستمر دست یابد.

سازمان باید موارد زیر را طرح‌ریزی کند:

د) اقدام‌هایی برای مقابله با این مخاطرات و فرصت‌ها؛ و

ه) چگونگی

۱. گنجاندن و پیاده‌سازی این اقدام‌ها در فرایندهای سیستم مدیریت امنیت اطلاعات سازمان؛ و

۲. ارزشیابی اثربخشی این اقدامات.

۲,۱,۶ ارزیابی مخاطرات امنیت اطلاعات

سازمان باید یک فرایند ارزیابی مخاطرات امنیت اطلاعات را تعریف نموده و به کار گیرد که:

الف) معیارهایی را برای مخاطرات امنیت اطلاعات، ایجاد و نگهداری کند که شامل موارد زیر باشد:

۱. معیارهای پذیرش مخاطرات؛ و

۲. معیارهایی برای انجام ارزیابی مخاطرات امنیت اطلاعات.

ب) اطمینان دهد که ارزیابی‌های مکرر مخاطرات امنیت اطلاعات، نتایج نامتناقض، معتبر و مقایسه‌پذیر تولید می‌کنند.

ج) مخاطرات امنیت اطلاعات را شناسایی کند:

۱. به کارگیری فرایند ارزیابی مخاطرات امنیت اطلاعات برای شناسایی مخاطرات مربوط به فقدان محرمانگی، صحت و دسترس‌پذیری اطلاعات در قلمرو سیستم مدیریت امنیت اطلاعات؛ و

۲. شناسایی مالکان مخاطره.

د) مخاطرات امنیت اطلاعات را تحلیل کند:

۱. ارزیابی پیامدهای احتمالی وقوع مخاطرات شناسایی شده در بند ۲,۱,۶ - ج - ۱؛

۲. ارزیابی احتمال واقع‌گرایانه وقوع مخاطرات شناسایی شده در بند ۲,۱,۶ - ج - ۱؛

۳. مشخص نمودن سطوح مخاطرات.

ه) مخاطرات امنیت اطلاعات را ارزشیابی کند:

۱. مقایسه نتایج تحلیل مخاطرات با معیارهای مخاطرات ایجاد شده در بند ۱,۲,۶ - الف؛ و

۲. اولویت‌بندی مخاطرات تحلیل شده برای برطرف‌سازی مخاطرات.

سازمان باید اطلاعاتی مستند درباره فرایند ارزیابی مخاطرات امنیت اطلاعات نگهداری کند.

۳,۱,۶ برطرف‌سازی مخاطرات امنیت اطلاعات

سازمان باید یک فرایند برطرف‌سازی مخاطرات امنیت اطلاعات را تعریف و اعمال کند تا بتواند:

الف) با درنظر گرفتن نتایج ارزیابی مخاطرات، گزینه‌های مناسب جهت برطرف‌سازی مخاطرات امنیت اطلاعات را انتخاب نماید.

ب) تمامی کنترل‌های ضروری به منظور پیاده‌سازی گزینه(های) انتخابی برطرف‌سازی مخاطرات امنیت اطلاعات را تعیین کند.

نکته: سازمان‌ها می‌توانند در صورت لزوم، کنترل‌هایی طراحی کنند یا آنها را از هر منبع دیگری شناسایی کنند.

ج) کنترل‌های تعیین شده در بند ۳,۱,۶ ب در بالا را با کنترل‌های موجود در پیوست الف، مقایسه کرده و بررسی کند که هیچ یک از کنترل‌های ضروری از قلم نیافتاده است.

نکته ۱: پیوست الف شامل فهرست جامعی از اهداف کنترلی و کنترل‌ها است. استفاده کنندگان از این استاندارد بین‌المللی برای حصول اطمینان از اینکه هیچ یک از کنترل‌های ضروری نادیده گرفته نشده است، به پیوست الف ارجاع داده می‌شوند.

نکته ۲: کنترل‌های انتخاب شده به طور ضمنی شامل اهداف کنترلی هستند. اهداف کنترلی و کنترل‌های فهرست شده در پیوست الف، جامع نبوده و ممکن است اهداف کنترلی و کنترل‌های اضافی هم مورد نیاز باشد.

د) یک بیانیه کاربست‌پذیری که شامل کنترل‌های ضروری (مراجعه به بند ۳,۱,۶ زیر بند ب و زیر بند ج) و دلیل استفاده از آنها بدون درنظر گرفتن اینکه پیاده‌سازی شده یا نشده‌اند و توجیه کنارگذاری کنترل‌های پیوست الف باشد، ایجاد نماید.

ه) یک طرح برطرف‌سازی مخاطرات امنیت اطلاعات را تدوین نماید؛ و

و) طرح برطرف‌سازی مخاطرات امنیت اطلاعات و پذیرش مخاطرات امنیت اطلاعات باقی‌مانده را از مالکان مخاطرات اخذ نماید.

سازمان باید اطلاعاتی مستند درباره فرایند برطرف‌سازی مخاطرات امنیت اطلاعات، نگهداری کند.

نکته: فرایند ارزیابی و برطرف‌سازی مخاطرات امنیت اطلاعات در این استاندارد بین‌المللی، با اصول و رهنمودهای کلی / عمومی موجود در ISO 31000[۵] مطابقت دارد.

۲,۶ اهداف امنیت اطلاعات و طرح‌ریزی برای دستیابی به آنها

سازمان باید اهداف امنیت اطلاعات را برای کارکردها و سطوح مرتبط ایجاد کند.

اهداف امنیت اطلاعات باید:

الف) با خط‌مشی امنیت اطلاعات، سازگار باشند.

ب) قابل اندازه‌گیری باشند (در صورت عملی بودن)؛

ج) الزامات قابل اجرای امنیت اطلاعات، و نتایج ارزیابی مخاطرات و نتایج برطرف‌سازی مخاطرات را درنظر بگیرند.

د) ابلاغ شوند؛ و

ه) در صورت نیاز، به روزرسانی شوند.

سازمان باید اطلاعاتی مستند را درباره اهداف امنیت اطلاعات، نگهداری کند.

سازمان باید هنگام طرح‌ریزی نحوه دستیابی به اهداف امنیت اطلاعات، موارد زیر را تعیین کند:

و) چه چیزی انجام خواهد شد.

ز) چه منابعی مورد نیاز خواهند بود.

ح) چه افرادی مسئول خواهند بود.

ط) چه زمانی تکمیل خواهد شد؛ و

ی) نتایج، چگونه ارزشیابی خواهند شد.

۷. پشتیبانی

۱,۷ منابع

سازمان باید منابع مورد نیاز به منظور استقرار، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات را تعیین و فراهم کند.

۲,۷ صلاحیت

سازمان باید:

الف) صلاحیت‌های مورد نیاز افرادی که تحت کنترل سازمان کار می‌کنند و بر روی عملکرد امنیت اطلاعات تأثیرگذار هستند را تعیین کند.

ب) اطمینان حاصل کند که این افراد، بر اساس تحصیلات، آموزش‌ها یا تجربیات مناسب، صلاحیت دارند.

ج) هر جا که امکان‌پذیر است، اقدام‌هایی را به منظور کسب صلاحیت لازم انجام داده و اثربخشی اقدام‌های انجام شده را ارزشیابی کند؛ و

د) اطلاعات مستند مناسب را به عنوان مدرکی مبنی بر صلاحیت، نگهداری کند.

نکته: اقدامات امکان‌پذیر، به طور مثال می‌توانند شامل ارایه آموزش، مشاوره یا جابجایی کارکنان فعلی، یا استخدام یا قرارداد با افراد شایسته باشد.

۳,۷ آگاه‌سازی

افرادی که تحت کنترل سازمان فعالیت می‌کنند باید نسبت به موارد زیر آگاه باشند:

الف) خط‌مشی امنیت اطلاعات؛

ب) سهم آنها در اثربخشی سیستم مدیریت امنیت اطلاعات، شامل منافع حاصل از بهبود عملکرد امنیت اطلاعات؛ و

ج) پیامدهای عدم انطباق با الزامات سیستم مدیریت امنیت اطلاعات.

۴,۷ ارتباطات

سازمان باید نیاز به ارتباطات درونی و بیرونی را در رابطه با سیستم مدیریت امنیت اطلاعات تعیین کند که شامل موارد زیر می‌شود:

الف) در چه زمینه‌ای ارتباط برقرار شود.

ب) چه زمانی ارتباط برقرار شود.

ج) با چه کسی ارتباط برقرار شود.

د) چه کسی باید ارتباط را برقرار کند؛ و

ه) فرایندهایی که ارتباط باید از طریق آن انجام شود.

۵,۷ اطلاعات مستند

۱,۵,۷ کلیات

سیستم مدیریت امنیت اطلاعات سازمان باید شامل این موارد باشد:

الف) اطلاعات مستند مورد نیاز این استاندارد بین‌المللی؛ و

ب) اطلاعات مستندی که از سوی سازمان برای اثربخشی سیستم مدیریت امنیت اطلاعات، ضروری تشخیص داده شده است.

نکته: گستره مستندسازی سیستم مدیریت امنیت اطلاعات می‌تواند به دلایل زیر برای هر سازمان متفاوت باشد:

۱. اندازه سازمان و نوع فعالیت‌ها، فرایندها، محصولات و خدمات آن؛

۲. پیچیدگی فرایندها و تعاملات آنها؛ و

۳. صلاحیت افراد.

۲,۵,۷ ایجاد و به روزرسانی

هنگام ایجاد و به روزرسانی اطلاعات مستند، سازمان باید از مناسب بودن موارد زیر اطمینان حاصل کند:

الف) شناسایی و توصیف (مثلاً یک عنوان، تاریخ، نگارنده یا شماره ارجاع)؛

ب) قالب (مثلاً زبان، نسخه نرم افزار، گرافیک) و رسانه (مثلاً کاغذی، الکترونیکی)؛ و

ج) بازنگری و تصویب جهت سازگاری و کفایت.

۳,۵,۷ کنترل اطلاعات مستند

اطلاعات مستند مورد نیاز سیستم مدیریت امنیت اطلاعات و این استاندارد بین‌المللی باید کنترل شوند تا اطمینان حاصل شود:

الف) در مکان و زمانی که برای استفاده، مورد نیاز هستند، در دسترس و مناسب هستند؛ و

ب) به میزان کافی حفاظت می‌شوند (به عنوان مثال در برابر فقدان محرمانگی، استفاده نادرست یا فقدان صحت).

به منظور کنترل اطلاعات مستند، سازمان باید در صورت قابلیت اجرا، فعالیت‌های زیر را مورد رسیدگی قرار دهد:

ج) توزیع، دسترسی، بازیابی و استفاده؛

د) ذخیره‌سازی و محافظت، شامل حفظ خوانایی؛

ه) کنترل تغییرات (برای مثال کنترل نسخه)؛ و

و) نگه‌داشتن و از بین بردن.

اطلاعات مستند با منشأ بیرونی که سازمان برای طرح‌ریزی و اجرای سیستم مدیریت امنیت اطلاعات ضروری تشخیص داده است باید به نحوی مناسب، شناسایی و کنترل شوند.

نکته: دسترسی به معنای تصمیم درباره صرفاً اجازه مشاهده اطلاعات مستند یا اجازه و اختیار جهت مشاهده و تغییر اطلاعات مستند و غیره است.

۸. عملیات

۱،۸ طرح‌ریزی و کنترل عملیات

سازمان باید فرایندهای مورد نیاز برای فراهم‌آوری الزامات امنیت اطلاعات را طرح‌ریزی، پیاده‌سازی و کنترل نموده و اقدام‌های مشخص شده در بند ۱،۶ را پیاده‌سازی کند. سازمان همچنین باید طرح‌هایی را برای دستیابی به اهداف امنیت اطلاعات مشخص شده در بند ۲،۶ پیاده‌سازی نماید.

سازمان باید اطلاعات مستند تا حدی ضروری را برای حصول اطمینان از اینکه فرایندها مطابق با طرح‌ها پیشروی داشته‌اند، نگهداری کند.

سازمان باید در صورت لزوم، اقدام‌هایی را برای کاهش هرگونه عوارض جانبی انجام دهد تا تغییرات طرح‌ریزی شده را کنترل و پیامدهای تغییرات ناخواسته را بازنگری نماید و سازمان باید اطمینان حاصل کند که فرایندهای برون‌سپاری شده، شناسایی و کنترل می‌شوند.

۲،۸ ارزیابی مخاطرات امنیت اطلاعات

سازمان باید ارزیابی مخاطرات امنیت اطلاعات را در بازه‌های زمانی طرح‌ریزی شده یا هنگام وقوع تغییرات مهم یا تغییرات پیشنهاد شده، با درنظر گرفتن معیار ایجاد شده در بند ۲،۱،۶ الف، انجام دهد.

سازمان باید اطلاعاتی مستند را درباره نتایج ارزیابی‌های مخاطرات امنیت اطلاعات، نگهداری کند.

۳،۸ برطرف‌سازی مخاطرات امنیت اطلاعات

سازمان باید طرح برطرف‌سازی مخاطرات امنیت اطلاعات را پیاده‌سازی کند.

سازمان باید اطلاعاتی مستند را درباره نتایج برطرف‌سازی مخاطرات امنیت اطلاعات، نگهداری کند.

۹. ارزشیابی عملکرد

۱,۹ پایش، اندازه‌گیری، تحلیل و ارزشیابی

سازمان باید عملکرد امنیت اطلاعات و اثربخشی سیستم مدیریت امنیت اطلاعات را ارزشیابی کند.

سازمان باید موارد زیر را مشخص کند:

الف) چه چیزهایی به پایش و اندازه‌گیری نیاز دارند، از جمله فرایندها و کنترل‌های امنیت اطلاعات؛

ب) در صورت قابلیت اعمال، روش‌هایی برای پایش، اندازه‌گیری، تحلیل و ارزشیابی، به منظور حصول اطمینان از معتبر بودن نتایج؛

نکته: روش‌های انتخابی باید نتایج قابل قیاس و تکرارپذیر تولید کنند تا معتبر شناخته شوند.

ج) چه زمانی باید پایش و اندازه‌گیری انجام شود.

د) چه کسی باید پایش و اندازه‌گیری را انجام دهد.

ه) چه زمانی نتایج حاصل از پایش و اندازه‌گیری باید مورد تحلیل و ارزشیابی قرار گیرند؛ و

و) چه کسی باید این نتایج را تحلیل و ارزشیابی کند.

سازمان باید اطلاعات مستند مناسب را به عنوان مدرک پایش و اندازه‌گیری نتایج، نگهداری کند.

۲,۹ ممیزی داخلی

سازمان باید ممیزی‌های داخلی را در فاصله‌های زمانی طرح‌ریزی شده انجام دهد تا اطلاع حاصل شود که آیا سیستم مدیریت امنیت اطلاعات:

الف) با موارد زیر انطباق دارد:

۱. الزامات خود سازمان برای سیستم مدیریت امنیت اطلاعات؛ و

۲. الزامات این استاندارد بین‌المللی؛

ب) به طور اثربخش، پیاده‌سازی و نگهداری می‌شود.

سازمان باید:

ج) برنامه(های) ممیزی شامل دفعات تکرار، روش‌ها، مسئولیت‌ها، الزامات طرح‌ریزی و گزارش‌دهی را طرح‌ریزی، مستقر، پیاده‌سازی و نگهداری کند. برنامه(های) ممیزی باید اهمیت فرایندهای مورد نظر و نتایج ممیزی‌های قبلی را درنظر بگیرند.

د) معیارهای ممیزی و قلمرو هر ممیزی را تعریف کند.

ه) در انتخاب ممیزان و انجام ممیزی‌ها، از واقع‌بینی و بی‌طرفی فرایند ممیزی اطمینان حاصل نماید.

و) اطمینان حاصل کند که نتایج ممیزی‌ها به مدیریت مربوطه گزارش داده می‌شوند؛ و

ز) اطلاعات مستند را به عنوان مدرک برنامه(های) ممیزی و نتایج ممیزی، نگهداری کند.

۳,۹ بازنگری مدیریت

مدیریت ارشد باید سیستم مدیریت امنیت اطلاعات سازمان را در فاصله‌های زمانی طرح‌ریزی شده، بازنگری کند تا از تداوم سازگاری، کفایت و اثربخشی آن اطمینان حاصل نماید.

در بازنگری مدیریت، باید موارد زیر درنظر گرفته شود:

الف) وضعیت اقدامات در بازنگری‌های قبلی مدیریت؛

ب) تغییرات در مسایل بیرونی و درونی مرتبط با سیستم مدیریت امنیت اطلاعات؛

ج) بازخوردها درباره عملکرد امنیت اطلاعات، شامل روند:

۱. عدم انطباق‌ها و اقدام‌های اصلاحی؛

۲. نتایج پایش و اندازه‌گیری؛

۳. نتایج ممیزی؛ و

۴. تحقق اهداف امنیت اطلاعات.

د) بازخورد از طرف‌های ذینفع؛

ه) نتایج ارزیابی مخاطرات و وضعیت طرح برطرف‌سازی مخاطرات؛ و

و) فرصت‌ها برای بهبود مستمر.

خروجی‌های بازنگری مدیریت باید دربرگیرنده تصمیمات مربوط به فرصت‌های بهبود مستمر و هرگونه نیاز به تغییر در سیستم مدیریت امنیت اطلاعات باشد.

سازمان باید اطلاعات مستند را به عنوان مدرک نتایج بازنگری‌های مدیریت، نگهداری کند.

۱۰. بهبود

۱,۱۰ عدم انطباق و اقدام اصلاحی

هنگام وقوع یک عدم انطباق، سازمان باید:

الف) نسبت به عدم انطباق، واکنش نشان داده و در صورت مقتضی:

۱. برای کنترل و اصلاح آن اقدام کند؛ و

۲. با پیامدهای آن مقابله کند.

ب) نیاز به اقدام برای رفع علل عدم انطباق را به منظور جلوگیری از تکرار یا بروز آن در جای دیگر، از طریق موارد زیر تعیین کند:

۱. بازنگری عدم انطباق؛

۲. تعیین علل عدم انطباق؛ و

۳. شناسایی وجود عدم انطباق‌های مشابه یا احتمال وقوع آنها.

ج) اقدام‌های مورد نیاز را پیاده‌سازی کند.

د) اثربخشی تمام اقدام‌های اصلاحی انجام شده را بازنگری کند؛ و

ه) در صورت لزوم، تغییراتی را در سیستم مدیریت امنیت اطلاعات ایجاد کند.

اقدام‌های اصلاحی باید متناسب با اثرات عدم انطباق‌های مشاهده شده باشند.

سازمان باید اطلاعات مستند را به عنوان مدرک برای موارد زیر نگهداری کند:

و) ماهیت عدم انطباق‌ها و تمام اقدام‌های انجام شده متعاقب آن؛ و

ز) نتایج هر یک از اقدام‌های اصلاحی.

۲,۱۰ بهبود مستمر

سازمان باید به طور مستمر، سازگاری، کفایت و اثربخشی سیستم مدیریت امنیت اطلاعات را بهبود بخشد.

پیوست الف

(الزامی)

کنترل‌ها و اهداف کنترلی مرجع

اهداف کنترلی و کنترل‌های فهرست شده در جدول الف.۱، به طور مستقیم از بندهای ۵ تا ۱۸ استاندارد [1] ISO/IEC 27002:2013 و منطبق با آنها برگرفته شده‌اند و در چارچوب بند ۳،۱،۶ مورد استفاده قرار خواهند گرفت.

جدول الف.۱ - اهداف کنترلی و کنترل‌ها

الف.۵: خط‌مشی‌های امنیت اطلاعات		
الف ۱،۵: هدایت مدیریت برای امنیت اطلاعات		
هدف: تأمین هدایت و پشتیبانی مدیریت از تطابق امنیت اطلاعات، مطابق با الزامات کسب و کار و قوانین و آیین‌نامه‌های مرتبط		
الف.۱،۱،۵	خط‌مشی‌های امنیت اطلاعات	کنترل: مجموعه‌ای از خط‌مشی‌های امنیت اطلاعات، باید تعریف و توسط مدیریت تصویب شود، منتشر شده و به اطلاع کارکنان و طرف‌های مرتبط بیرونی برسد.
الف.۲،۱،۵	بازنگری خط‌مشی‌های امنیت اطلاعات	کنترل: خط‌مشی‌های امنیت اطلاعات باید در فواصل زمانی طرح‌ریزی شده یا در صورتی که تغییرات مهمی رخ دهد، به منظور حصول اطمینان از تداوم سازگاری، کفایت و اثربخشی آنها بازنگری شوند.
الف.۶: سازمان امنیت اطلاعات		
الف.۱،۶: سازمان داخلی		
هدف: ایجاد یک چارچوب امنیتی به منظور شروع و کنترل پیاده‌سازی و اجرای امنیت اطلاعات در درون سازمان		
الف.۱،۱،۶	نقش‌ها و مسئولیت‌های امنیت اطلاعات	کنترل: کلیه مسئولیت‌های امنیت اطلاعات، باید تعریف و محول شوند.
الف.۲،۱،۶	تفکیک وظایف	کنترل: به منظور کاهش فرصت‌های دستکاری غیرمجاز یا غیرعمد، یا سوءاستفاده از دارایی‌های سازمان، باید وظایف و حدود مسئولیت‌های مغایر، تفکیک شوند.
الف.۳،۱،۶	ارتباط با مراجع معتبر	کنترل: ارتباطات مقتضی با مراجع معتبر مرتبط باید حفظ شود.
الف.۴،۱،۶	ارتباط با گروه‌های ذینفع ویژه	کنترل: ارتباطات مقتضی با گروه‌های ذینفع ویژه یا سایر انجمن‌های امنیتی متخصص و انجمن‌های حرفه‌ای باید حفظ شود.
الف.۵،۱،۶	امنیت اطلاعات در مدیریت پروژه	کنترل: امنیت اطلاعات باید در مدیریت پروژه، صرف‌نظر از نوع پروژه، لحاظ شود.
الف.۲،۶: دستگاه‌های قابل حمل و دورکاری		
هدف: حصول اطمینان از امنیت دورکاری و استفاده از دستگاه‌های قابل حمل		
الف.۱،۲،۶	خط‌مشی دستگاه‌های قابل حمل	کنترل: یک خط‌مشی و اقدامات امنیتی پشتیبان، به منظور مدیریت مخاطرات ایجاد شده به دلیل استفاده از دستگاه‌های قابل حمل، باید اتخاذ گردد.
الف.۲،۲،۶	دورکاری	کنترل: یک خط‌مشی و اقدامات امنیتی پشتیبان، به منظور حفاظت از اطلاعات قابل

		دسترس، پردازش یا ذخیره شده در محل‌های دورکاری، باید پیاده‌سازی شود.
الف.۷: امنیت منابع انسانی		
الف.۱،۷: پیش از اشتغال		
هدف: حصول اطمینان از اینکه کارکنان و پیمانکاران، مسئولیت‌هایشان را درک کرده و برای نقش‌های درنظر گرفته شده برای ایشان مناسب هستند.		
الف.۱،۱،۷	گزینش	کنترل: پیشینه تمام داوطلبان استخدام، باید مطابق با قوانین مرتبط، آیین‌نامه‌ها و اصول اخلاقی، بررسی گردد و متناسب با الزامات کسب و کار، طبقه‌بندی اطلاعاتی که در دسترس قرار می‌گیرند و مخاطرات بالقوه باشند.
الف.۲،۱،۷	ضوابط و شرایط استخدام	کنترل: توافق‌های قراردادی با کارکنان و پیمانکاران باید بیانگر مسئولیت‌های ایشان و سازمان، در قبال امنیت اطلاعات باشد.
الف.۲،۷: حین خدمت		
هدف: حصول اطمینان از اینکه کارکنان و پیمانکاران از مسئولیت‌های امنیت اطلاعات خود، آگاه بوده و آنها را به انجام می‌رسانند.		
الف.۱،۲،۷	مسئولیت‌های مدیریت	کنترل: مدیریت باید تمامی کارکنان و پیمانکاران را به بکارگیری امنیت اطلاعات، مطابق با خط‌مشی‌ها و رویه‌های ایجاد شده سازمان، الزام نماید.
الف.۲،۲،۷	آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات	کنترل: تمامی کارکنان سازمان، و در صورت لزوم پیمانکاران، باید به صورت مناسب، در خصوص خط‌مشی‌ها و رویه‌های سازمان، تحصیل و آموزش آگاه‌سازانه ببینند و به طور منظم به روز شوند، به طوری که به کارکرد شغلی ایشان مرتبط باشد.
الف.۳،۲،۷	فرایند انضباطی	کنترل: باید برای اقدام در برابر کارکنانی که مرتکب نقض امنیت اطلاعات شده‌اند یک فرایند انضباطی رسمی و ابلاغ شده، وجود داشته باشد.
الف.۳،۷: خاتمه اشتغال یا تغییر شغل		
هدف: محافظت از منافع سازمان، به عنوان بخشی از فرایند تغییر یا خاتمه اشتغال		
الف.۱،۳،۷	مسئولیت‌های خاتمه اشتغال یا تغییر شغل	کنترل: مسئولیت‌ها و وظایف امنیت اطلاعات که پس از خاتمه اشتغال یا تغییر شغل، معتبر باقی می‌مانند باید تعریف شده، به کارکنان یا پیمانکاران ابلاغ و اجبار شوند.
الف.۸: مدیریت دارایی‌ها		
الف.۱،۸: مسئولیت دارایی‌ها		
هدف: شناسایی دارایی‌های سازمانی و تعریف مسئولیت‌های حفاظت مناسب		
الف.۱،۱،۸	سیاهه اموال	کنترل: دارایی‌های مرتبط با اطلاعات و امکانات پردازش اطلاعات باید شناسایی شده و سیاهه‌ای از این دارایی‌ها تنظیم و نگهداری شود.
الف.۲،۱،۸	مالکیت دارایی‌ها	کنترل: دارایی‌های نگهداری شده در سیاهه باید دارای مالک باشند.
الف.۳،۱،۸	استفاده پسندیده از دارایی‌ها	کنترل: قوانینی برای استفاده پسندیده از اطلاعات و دارایی‌های مرتبط با اطلاعات و امکانات پردازش اطلاعات، باید شناسایی، مدون و پیاده‌سازی شوند.
الف.۴،۱،۸	عودت دارایی‌ها	کنترل: تمامی کارکنان و کاربران طرف بیرونی باید کلیه دارایی‌های سازمانی را که در اختیار دارند، به محض خاتمه اشتغال، قرارداد یا توافق‌نامه، عودت دهند.
الف.۲،۸: طبقه‌بندی اطلاعات		
هدف: حصول اطمینان از اینکه اطلاعات، با توجه به اهمیت آن برای سازمان، به سطح حفاظتی مناسب رسیده است.		
الف.۱،۲،۸	طبقه‌بندی اطلاعات	کنترل: اطلاعات باید با توجه به الزامات قانونی، ارزش، بحرانی بودن و حساس بودن

		نسبت به افشا یا دستکاری غیرمجاز، طبقه‌بندی شوند.
الف.۸.۲،۲	برچسب گذاری اطلاعات	کنترل: باید مجموعه مناسبی از رویه‌هایی برای برچسب گذاری اطلاعات، با توجه به الگوی طبقه‌بندی اطلاعات پذیرفته شده توسط سازمان، ایجاد و پیاده‌سازی شود.
الف.۸.۳،۲	اداره کردن دارایی	کنترل: باید رویه‌هایی برای اداره کردن دارایی‌ها، با توجه به الگوی طبقه‌بندی اطلاعات پذیرفته شده توسط سازمان، ایجاد و پیاده‌سازی شود.
الف.۸.۳: اداره کردن رسانه‌ها		
هدف: پیشگیری از افشا، دستکاری، حذف یا تخریب غیرمجاز اطلاعات ذخیره شده در رسانه‌ها		
الف.۸.۱،۳	مدیریت رسانه‌های جداشدنی	کنترل: باید رویه‌هایی برای مدیریت رسانه‌های جداشدنی، با توجه به الگوی طبقه بندی پذیرفته شده توسط سازمان، ایجاد و پیاده‌سازی شود.
الف.۸.۲،۳	امحاء رسانه	کنترل: رسانه‌ها باید زمانی که دیگر مورد نیاز نیستند، به صورت امن و با استفاده از رویه‌هایی رسمی، امحا شوند.
الف.۸.۳،۳	انتقال رسانه فیزیکی	کنترل: رسانه‌های حاوی اطلاعات باید در حین انتقال، در برابر دسترسی غیرمجاز، سوءاستفاده یا خرابی، محافظت شوند.
الف.۹: کنترل دسترسی		
الف.۹.۱: الزامات کسب و کار برای کنترل دسترسی		
هدف: محدودسازی دسترسی به اطلاعات و امکانات پردازش اطلاعات		
الف.۹.۱،۱	خط‌مشی کنترل دسترسی	کنترل: باید خط‌مشی کنترل دسترسی، بر مبنای الزامات کسب و کار و امنیت اطلاعات، ایجاد، مدون و بازنگری شود.
الف.۹.۱،۲	دسترسی به شبکه‌ها و سرویس‌های شبکه	کنترل: کاربران فقط باید به شبکه و سرویس‌هایی از شبکه دسترسی داشته باشند که بطور مشخص، مجوز استفاده از آنها را داشته باشند.
الف.۹.۲: مدیریت دسترسی کاربر		
هدف: حصول اطمینان از دسترسی کاربر مجاز شده و جلوگیری از دسترسی غیرمجاز به سیستم‌ها و سرویس‌ها		
الف.۹.۱،۲	ثبت و حذف کاربر	کنترل: باید فرایندی رسمی برای ثبت و حذف کاربر، به منظور ایجاد امکان اعطای حقوق دسترسی، پیاده‌سازی شود.
الف.۹.۲،۲	تأمین مجوز دسترسی کاربر	کنترل: باید یک فرایند رسمی تأمین مجوز دسترسی کاربر، جهت اعطا یا لغو حقوق دسترسی برای کلیه انواع کاربران به تمامی سیستم‌ها و سرویس‌ها، پیاده‌سازی شود.
الف.۹.۳،۲	مدیریت حق دسترسی ویژه	کنترل: تخصیص و به کارگیری حق دسترسی ویژه، باید محدود و کنترل شود.
الف.۹.۴،۲	مدیریت اطلاعات محرمانه احراز هویت کاربران	کنترل: تخصیص اطلاعات محرمانه احراز هویت، باید از طریق یک فرایند رسمی مدیریتی، کنترل شود.
الف.۹.۵،۲	بازنگری حقوق دسترسی کاربر	کنترل: مالکان دارایی‌ها باید حقوق دسترسی کاربران را در فواصل زمانی منظم بازنگری کنند.
الف.۹.۶،۲	حذف یا اصلاح حقوق دسترسی	کنترل: حقوق دسترسی تمامی کارکنان و کاربران طرف بیرونی به اطلاعات و امکانات پردازش اطلاعات، باید به محض خاتمه اشتغال، قرارداد یا توافق‌نامه آنها حذف شده، و در صورت تغییر وضعیت، اصلاح شوند.
الف.۹.۳: مسئولیت‌های کاربر		
هدف: پاسخگو بودن کاربران در برابر حفاظت از اطلاعات احراز هویت خود		

الف.۱,۳,۹	استفاده از اطلاعات محرمانه احراز هویت	کنترل: کاربران باید به پیروی از دستورالعمل‌های سازمانی جهت استفاده از اطلاعات محرمانه احراز هویت، ملزم شوند.
الف.۴,۹: کنترل دسترسی به سیستم و برنامه		
هدف: جلوگیری از دسترسی غیرمجاز به سیستم‌ها و برنامه‌ها		
الف.۱,۴,۹	محدودیت دسترسی به اطلاعات	کنترل: دسترسی به اطلاعات و کارکردهای سیستم برنامه، باید مطابق با خط‌مشی کنترل دسترسی، محدود شود.
الف.۲,۴,۹	رویه‌های ورود امن	کنترل: دسترسی به سیستم‌ها و برنامه‌ها، در صورت الزام در خط‌مشی کنترل دسترسی، باید توسط یک رویه ورود امن، کنترل شود.
الف.۳,۴,۹	سیستم مدیریت کلمه عبور	کنترل: سیستم‌های مدیریت کلمه عبور باید تعاملی بوده و کیفیت کلمات عبور را تضمین نمایند.
الف.۴,۴,۹	استفاده از برنامه‌های کمکی ویژه	کنترل: استفاده از برنامه‌های کمکی که ممکن است قادر به ابطال کنترل‌های سیستم و برنامه‌ها باشند، باید محدود شده و به شدت کنترل شود.
الف.۵,۴,۹	کنترل دسترسی به کد منبع برنامه	کنترل: دسترسی به کد منبع برنامه، باید محدود شود.
الف.۱۰: رمزنگاری		
الف.۱,۱۰: کنترل‌های رمزنگاری		
هدف: حصول اطمینان از استفاده بجا و اثربخش از رمزنگاری، به منظور حفاظت از محرمانگی، اصالت یا صحت اطلاعات		
الف.۱,۱,۱۰	خط‌مشی استفاده از کنترل های رمزنگاری	کنترل: باید خط‌مشی استفاده از کنترل‌های رمزنگاری، برای حفاظت از اطلاعات، ایجاد و پیاده‌سازی شود.
الف.۲,۱,۱۰	مدیریت کلید	کنترل: خط‌مشی استفاده، حفاظت و طول عمر کلیدهای رمزنگاری، باید ایجاد و در کل چرخه حیات آنها پیاده‌سازی شود.
الف.۱۱: امنیت فیزیکی و محیطی		
الف.۱,۱۱: نواحی امن		
هدف: جلوگیری از دسترسی فیزیکی غیرمجاز، خسارت و مداخله در اطلاعات و امکانات پردازش اطلاعات سازمان		
الف.۱,۱,۱۱	حصار امنیت فیزیکی	کنترل: حصارهای امنیتی باید برای حفاظت از نواحی حاوی اطلاعات و امکانات پردازش اطلاعات حساس یا حیاتی، تعیین شده و استفاده شوند.
الف.۲,۱,۱۱	کنترل‌های مداخل فیزیکی	کنترل: نواحی امن، به منظور حصول اطمینان از اینکه فقط کارکنان مجاز، اجازه دسترسی دارند، باید توسط کنترل‌های مداخل مناسب، حفاظت شوند.
الف.۳,۱,۱۱	امن‌سازی دفاتر، اتاق‌ها و امکانات	کنترل: امنیت فیزیکی برای دفاتر، اتاق‌ها و امکانات، باید طراحی شده و به کار گرفته شود.
الف.۴,۱,۱۱	محافظت در برابر تهدیدهای بیرونی و محیطی	کنترل: حفاظت فیزیکی در برابر بلایای طبیعی، سوانح و حملات خرابکارانه، باید طراحی شده و به کار گرفته شود.
الف.۵,۱,۱۱	نواحی تحویل و بارگیری	کنترل: نقاط دسترسی مانند نواحی تحویل و بارگیری و سایر نقاطی که افراد متفرقه ممکن است وارد محوطه‌ها شوند، باید تحت کنترل قرار گیرند، و در صورت امکان، برای جلوگیری از دسترسی غیرمجاز، از امکانات پردازش اطلاعات، مجزا شوند.
الف.۲,۱۱: تجهیزات		

هدف: جلوگیری از فقدان، آسیب، سرقت یا به خطر افتادن دارایی‌ها و ایجاد وقفه در فعالیت‌های سازمان		
الف.۱,۲,۱۱	استقرار و حفاظت از تجهیزات	کنترل: تجهیزات باید (در محل مناسب) مستقر و محافظت شوند تا مخاطرات ناشی از تهدیدها و خطرات محیطی و فرصت‌های دسترسی غیرمجاز، کاهش یابند.
الف.۲,۲,۱۱	امکانات پشتیبانی	کنترل: تجهیزات باید در برابر خرابی برق و سایر اختلالات ناشی از خرابی امکانات پشتیبانی، محافظت شوند.
الف.۳,۲,۱۱	امنیت کابل‌کشی	کنترل: کابل‌کشی‌های برق و مخابرات مورد استفاده برای انتقال داده یا پشتیبانی از سرویس‌های اطلاعاتی، باید در برابر قطع شدن، ایجاد تداخل یا آسیب، محافظت شوند.
الف.۴,۲,۱۱	نگهداری تجهیزات	کنترل: تجهیزات باید به منظور حصول اطمینان از تداوم دسترس‌پذیری و صحت‌شان، به درستی نگهداری شوند.
الف.۵,۲,۱۱	خروج دارایی‌ها	کنترل: تجهیزات، اطلاعات یا نرم افزار، نباید بدون مجوز قبلی از محل خارج شوند.
الف.۶,۲,۱۱	امنیت تجهیزات و دارایی‌های خارج از محوطه	کنترل: برای دارایی‌های خارج از محوطه، باید با توجه به مخاطرات مختلف ناشی از انجام کار در خارج از محوطه‌های سازمان، امنیت برقرار شود.
الف.۷,۲,۱۱	امحا یا استفاده مجدد از تجهیزات به صورت امن	کنترل: تمام اجزای تجهیزاتی که دارای رسانه ذخیره‌سازی هستند، باید به منظور حصول اطمینان از اینکه کلیه داده‌های حساس و نرم افزارهای دارای حق امتیاز، پیش از امحا یا استفاده مجدد، حذف شده یا به شیوه امنی بازنویسی شده‌اند، بررسی شوند.
الف.۸,۲,۱۱	تجهیزات بدون مراقبت کاربر	کنترل: کاربران باید اطمینان حاصل کنند که تجهیزات بدون مراقبت، حفاظت مناسبی دارند.
الف.۹,۲,۱۱	خط‌مشی میز پاک و صفحه پاک	کنترل: خط‌مشی میز پاک برای اوراق و رسانه‌های ذخیره‌سازی جداشدنی، و خط‌مشی صفحه پاک برای امکانات پردازش اطلاعات، باید اتخاذ شود.
الف.۱۲: امنیت عملیات		
الف.۱,۱۲: رویه‌های عملیاتی و مسئولیت‌ها		
هدف: حصول اطمینان از کارکرد صحیح و امن امکانات پردازش اطلاعات		
الف.۱,۱,۱۲	رویه‌های عملیاتی مدون	کنترل: رویه‌های عملیاتی باید مدون شوند و در دسترس همه کاربرانی که به آنها نیاز دارند، قرار گیرند.
الف.۲,۱,۱۲	مدیریت تغییر	کنترل: تغییرات در سازمان، فرایندهای کسب و کار، امکانات و سیستم‌های پردازش اطلاعات که بر امنیت اطلاعات تأثیرگذار هستند، باید کنترل شوند.
الف.۳,۱,۱۲	مدیریت ظرفیت	کنترل: استفاده از منابع، باید پایش و تنظیم شده و پیش‌بینی ظرفیت مورد نیاز آینده جهت حصول اطمینان از کارایی الزامات سیستم، انجام شود.
الف.۴,۱,۱۲	جداسازی محیط‌های توسعه، آزمایش و عملیاتی	کنترل: محیط‌های توسعه، آزمایش و عملیاتی، باید به منظور کاهش مخاطرات ناشی از دسترسی یا تغییر غیرمجاز در محیط عملیاتی، از یکدیگر جدا شوند.
الف.۲,۱۲: حفاظت در برابر بدافزارها		
هدف: حصول اطمینان از اینکه اطلاعات و امکانات پردازش اطلاعات در برابر بدافزارها حفاظت می‌شوند.		
الف.۱,۲,۱۲	کنترل‌ها در برابر بدافزارها	کنترل: کنترل‌های تشخیص، جلوگیری و بازیابی، به منظور حفاظت در برابر بدافزارها، باید پیاده‌سازی شده و با آگاه‌سازی مناسب کاربر همراه شوند.
الف.۳,۱۲: پشتیبان‌گیری		

هدف: حفاظت در برابر فقدان داده‌ها		
الف.۱,۳,۱۲	پشتیبان‌گیری از اطلاعات	کنترل: نسخه‌های پشتیبان از اطلاعات، نرم افزار و تصاویر سیستم، باید با توجه به خط‌مشی مورد توافق پشتیبان‌گیری، تهیه و به صورت منظم آزمایش شوند.
الف.۴,۱۲: ثبت و پایش		
هدف: ثبت رویدادها و ایجاد شواهد		
الف.۱,۴,۱۲	ثبت رویداد	کنترل: ثبت رویدادها شامل ثبت فعالیت‌های کاربر، استثناءها، خطاها و رویدادهای امنیت اطلاعات، باید ایجاد، نگهداری و به صورت منظم بازنگری شوند.
الف.۲,۴,۱۲	حفاظت از اطلاعات ثبت شده رویدادها	کنترل: امکانات ثبت رویداد و اطلاعات ثبت شده، باید در برابر دستکاری و دسترسی غیرمجاز حفاظت شوند.
الف.۳,۴,۱۲	ثبت رویدادهای مدیر و اپراتور سیستم	کنترل: فعالیت‌های مدیر سیستم و اپراتور سیستم باید ثبت شوند و رویدادهای ثبت شده باید محافظت و به صورت منظم، بازنگری شوند.
الف.۴,۴,۱۲	همزمان‌سازی ساعت‌ها	کنترل: ساعت‌های تمامی سیستم‌های پردازش اطلاعات مرتبط در درون یک سازمان یا دامنه اطلاعاتی، باید با یک منبع زمانی مرجع واحد، همزمان شوند.
الف.۵,۱۲: کنترل نرم افزارهای عملیاتی		
هدف: حصول اطمینان از صحت سیستم‌های عملیاتی		
الف.۱,۵,۱۲	نصب نرم افزار بر روی سیستم های عملیاتی	کنترل: رویه‌هایی برای کنترل نصب نرم افزار بر روی سیستم‌های عملیاتی باید پیاده سازی شوند.
الف.۶,۱۲: مدیریت آسیب‌پذیری فنی		
هدف: جلوگیری از بهره‌برداری از آسیب‌پذیری‌های فنی		
الف.۱,۶,۱۲	مدیریت آسیب‌پذیری‌های فنی	کنترل: اطلاعات در خصوص آسیب‌پذیری‌های فنی سیستم‌های اطلاعاتی مورد استفاده، باید به موقع کسب شود، قرارگیری سازمان در معرض چنین آسیب‌پذیری هایی ارزیابی شده و اقدامات مناسبی برای مقابله با مخاطرات مربوطه انجام شود.
الف.۲,۶,۱۲	محدودیت‌هایی برای نصب نرم افزار	کنترل: برای کنترل نصب نرم افزار توسط کاربران، باید قوانینی ایجاد و پیاده‌سازی شود.
الف.۷,۱۲: ملاحظات ممیزی سیستم‌های اطلاعاتی		
هدف: به حداقل رساندن تأثیر فعالیت‌های ممیزی بر سیستم‌های عملیاتی		
الف.۱,۷,۱۲	کنترل‌های ممیزی سیستم های اطلاعاتی	کنترل: الزامات و فعالیت‌های ممیزی مرتبط با بررسی سیستم‌های عملیاتی، باید به دقت طرح‌ریزی شده و مورد توافق قرار گیرند تا ایجاد وقفه در فرایندهای کسب و کار به حداقل برسد.
الف.۱۳: امنیت ارتباطات		
الف.۱,۱۳: مدیریت امنیت شبکه		
هدف: حصول اطمینان از حفاظت اطلاعات در شبکه‌ها و امکانات پردازش اطلاعات پشتیبان آنها		
الف.۱,۱,۱۳	کنترل‌های شبکه	کنترل: شبکه‌ها باید مدیریت و کنترل شوند تا از اطلاعات درون سیستم‌ها و برنامه‌ها محافظت شود.
الف.۲,۱,۱۳	امنیت سرویس‌های شبکه	کنترل: سازوکارهای امنیتی، سطوح خدمات و الزامات مدیریتی تمامی سرویس‌های شبکه، باید شناسایی شده و چه این سرویس‌ها به صورت درون سازمانی تأمین و چه

		برون‌سپاری شده‌اند، در توافق‌نامه‌های سرویس‌های شبکه لحاظ شوند.
الف.۳,۱,۱۳	تفکیک شبکه‌ها	کنترل: گروه‌های سرویس‌های اطلاعاتی، کاربران و سیستم‌های اطلاعاتی، باید در شبکه‌ها تفکیک شوند.
الف.۲,۱۳: انتقال اطلاعات		
هدف: حفظ امنیت اطلاعات منتقل شده درون سازمانی، با هر یک از موجودیت‌های بیرونی		
الف.۱,۲,۱۳	خط‌مشی‌ها و رویه‌های انتقال اطلاعات	کنترل: برای حفاظت از انتقال اطلاعات به واسطه استفاده از تمامی انواع امکانات ارتباطی، باید خط‌مشی‌ها، رویه‌ها و کنترل‌های رسمی انتقال، تعیین شوند.
الف.۲,۲,۱۳	توافق‌نامه‌های انتقال اطلاعات	کنترل: توافق‌نامه‌ها باید انتقال اطلاعات کسب و کار را به صورت امن، مابین سازمان و طرف‌های بیرونی، لحاظ کنند.
الف.۳,۲,۱۳	پیام‌رسانی الکترونیکی	کنترل: اطلاعات درگیر در پیام‌رسانی الکترونیکی، باید به صورت مناسبی حفاظت شوند.
الف.۴,۲,۱۳	توافق‌نامه‌های محرمانگی یا عدم افشا	کنترل: الزامات توافق‌نامه‌های محرمانگی یا عدم افشا که منعکس کننده نیازهای سازمان به منظور حفاظت از اطلاعات هستند، باید تعیین شده و به صورت منظم بازنگری و مدون شوند.
الف.۱۴: اکتساب، توسعه و نگهداری از سیستم		
الف.۱,۱۴: الزامات امنیتی سیستم‌های اطلاعاتی		
هدف: حصول اطمینان از اینکه امنیت اطلاعات، یک جزء جدایی‌ناپذیر از سیستم‌های اطلاعاتی در طول کل چرخه حیات است. این موضوع شامل الزاماتی برای سیستم‌های اطلاعاتی که تأمین کننده سرویس‌هایی بر روی شبکه‌های عمومی هستند نیز می‌شود.		
الف.۱,۱,۱۴	تحلیل و تعیین الزامات امنیت اطلاعات	کنترل: الزامات مربوط به امنیت اطلاعات باید در الزامات سیستم‌های اطلاعاتی جدید یا گسترش سیستم‌های اطلاعاتی موجود لحاظ شوند.
الف.۲,۱,۱۴	ایمن‌سازی سرویس‌های برنامه بر روی شبکه‌های عمومی	کنترل: اطلاعات درگیر در سرویس‌های برنامه که بر روی شبکه‌های عمومی منتقل می‌شوند باید در برابر فعالیت‌های متقلبانه، اختلافات قرارداد، دستکاری و افشای غیرمجاز محافظت شوند.
الف.۳,۱,۱۴	حفاظت از تراکنش‌های سرویس‌های برنامه	کنترل: اطلاعات درگیر در تراکنش‌های سرویس برنامه، به منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه، تغییر غیرمجاز پیام، افشای غیرمجاز و تکرار یا پاسخ‌دهی غیرمجاز به پیام باید محافظت شوند.
الف.۲,۱۴: امنیت در فرایندهای توسعه و پشتیبانی		
هدف: حصول اطمینان از اینکه امنیت اطلاعات، در درون چرخه حیات سیستم‌های اطلاعاتی، طراحی و پیاده‌سازی شده است.		
الف.۱,۲,۱۴	خط‌مشی توسعه امن	کنترل: برای توسعه نرم افزار و سیستم‌ها، باید قوانینی وضع شده و در توسعه‌های درون سازمان به کار گرفته شود.
الف.۲,۲,۱۴	رویه‌های کنترل تغییر سیستم	کنترل: تغییرات بر روی سیستم‌ها در طول چرخه حیات توسعه باید با استفاده از رویه های رسمی کنترل تغییر، کنترل شوند.
الف.۳,۲,۱۴	بازنگری فنی برنامه‌ها پس از تغییرات بسترهای عملیاتی	کنترل: هنگام تغییر بسترهای عملیاتی، برنامه‌های حیاتی کسب و کار باید بازنگری و آزمایش شوند تا از عدم وجود تأثیر سوء بر عملیات یا امنیت سازمانی، اطمینان حاصل شود.
الف.۴,۲,۱۴	محدودسازی در اعمال تغییر در بسته‌های نرم افزاری	کنترل: دستکاری در بسته‌های نرم افزاری باید مسدود شده و محدود به تغییرات ضروری باشد و تمامی تغییرات باید به شدت کنترل شوند.

الف.۵,۲,۱۴	اصول مهندسی سیستم‌های امن	کنترل: اصولی برای مهندسی سیستم‌های امن، باید وضع، مدون و نگهداری شده و در تمام فعالیت‌ها برای پیاده‌سازی سیستم‌های اطلاعاتی به کار گرفته شود.
الف.۶,۲,۱۴	محیط توسعه امن	کنترل: سازمان‌ها باید برای توسعه سیستم و فعالیت‌های یکپارچه‌سازی که کل چرخه حیات توسعه سیستم را دربرمی‌گیرند، محیط‌های توسعه امن را ایجاد کرده و به شیوه مناسبی از آنها محافظت کنند.
الف.۷,۲,۱۴	توسعه برون‌سپاری شده	کنترل: فعالیت توسعه سیستم برون‌سپاری شده، باید توسط سازمان، نظارت و پایش شود.
الف.۸,۲,۱۴	آزمون امنیت سیستم	کنترل: آزمون عملکرد امنیتی باید در طول توسعه آزمایش شود.
الف۳,۱۴: داده‌های آزمون		
هدف: حصول اطمینان از حفاظت داده‌های مورد استفاده برای آزمون		
الف.۱,۳,۱۴	حفاظت از داده‌های آزمون	کنترل: داده‌های آزمون باید به دقت انتخاب، محافظت و کنترل شوند.
الف.۱۵: روابط تأمین کنندگان		
الف.۱,۱۵: امنیت اطلاعات در روابط با تأمین کنندگان		
هدف: حصول اطمینان از حفاظت آن دسته از دارایی‌های سازمان که در دسترس تأمین کنندگان قرار دارند.		
الف.۱,۱,۱۵	خط‌مشی امنیت اطلاعات برای ارتباط با تأمین کنندگان	کنترل: الزامات امنیت اطلاعات برای کاهش مخاطرات ناشی از دسترسی تأمین کنندگان به دارایی‌های سازمان، باید مورد توافق تأمین کنندگان قرار گرفته و مدون شوند.
الف.۲,۱,۱۵	لحاظ کردن امنیت در توافق نامه‌های تأمین کنندگان	کنترل: کلیه الزامات مرتبط با امنیت اطلاعات، باید با هر یک از تأمین کنندگانی که امکان دسترسی، پردازش، ذخیره‌سازی، ارتباط یا تأمین اجزای زیرساخت فناوری اطلاعات سازمان را دارند مشخص گردد و مورد توافق آنها قرار گیرد.
الف.۳,۱,۱۵	زنجیره تأمین فناوری اطلاعات و ارتباطات	کنترل: توافق‌نامه‌ها با تأمین کنندگان باید دربرگیرنده الزاماتی برای مقابله با مخاطرات امنیت اطلاعات ناشی از زنجیره تأمین محصولات و خدمات فناوری اطلاعات و ارتباطات باشند.
الف.۲,۱۵: مدیریت تحویل خدمت تأمین کنندگان		
هدف: حفظ یک سطح مورد توافق برای امنیت اطلاعات و تحویل خدمات، مطابق با توافق‌نامه‌های تأمین کنندگان		
الف.۱,۲,۱۵	پایش و بازنگری خدمات تأمین کنندگان	کنترل: سازمان‌ها باید تحویل خدمات تأمین کنندگان را به صورت منظم پایش، بازنگری و ممیزی کنند.
الف.۲,۲,۱۵	مدیریت تغییرات در خدمات تأمین کنندگان	کنترل: تغییرات در تهیه خدمات توسط تأمین کنندگان، شامل نگهداری و بهبود خط مشی‌ها، رویه‌ها و کنترل‌های امنیت اطلاعات موجود، باید با توجه به بحرانی بودن اطلاعات کسب و کار، سیستم‌ها و فرایندهای موجود و ارزیابی مجدد مخاطرات، مدیریت شوند.
الف.۱۶: مدیریت رخدادهای امنیت اطلاعات		
الف.۱,۱۶: مدیریت و بهبود رخدادهای امنیت اطلاعات		
هدف: حصول اطمینان از بکارگیری رویکردی استوار و اثربخش برای مدیریت رخدادهای امنیت اطلاعات، شامل اعلان رویدادهای امنیتی و نقاط ضعف		
الف.۱,۱,۱۶	مسئولیت‌ها و رویه‌ها	کنترل: مسئولیت‌های مدیریتی و رویه‌ها، به منظور حصول اطمینان از پاسخگویی

		سریع، مؤثر و منظم به رخدادهای امنیت اطلاعات، باید وضع شوند.
الف.۲,۱,۱۶	گزارش‌دهی رویدادهای امنیت اطلاعات	کنترل: رویدادهای امنیت اطلاعات باید از طریق مجاری مدیریتی مناسب، در کوتاه ترین زمان ممکن گزارش شوند.
الف.۳,۱,۱۶	گزارش‌دهی نقاط ضعف امنیت اطلاعات	کنترل: کارکنان و پیمانکارانی که از سیستم‌ها و سرویس‌های اطلاعاتی سازمان استفاده می‌کنند، باید نسبت به یادداشت‌برداری و گزارش‌دهی هرگونه ضعف امنیت اطلاعات مشاهده شده یا مشکوک در سیستم‌ها یا سرویس‌ها، ملزم شوند.
الف.۴,۱,۱۶	ارزیابی و تصمیم‌گیری درباره رویدادهای امنیت اطلاعات	کنترل: رویدادهای امنیت اطلاعات، باید ارزیابی شوند و در خصوص اینکه لازم است به عنوان رخدادهای امنیت اطلاعات طبقه‌بندی شوند، تصمیم‌گیری شود.
الف.۵,۱,۱۶	پاسخ به رخدادهای امنیت اطلاعات	کنترل: باید به توجه به رویه‌های مدون، به رخدادهای امنیت اطلاعات پاسخ داده شود.
الف.۶,۱,۱۶	یادگیری از رخدادهای امنیت اطلاعات	کنترل: دانش کسب شده از تحلیل و رفع رخدادهای امنیت اطلاعات، باید برای کاهش احتمال یا اثر رخدادها در آینده، مورد استفاده قرار گیرد.
الف.۷,۱,۱۶	جمع‌آوری شواهد	کنترل: سازمان باید رویه‌هایی را برای شناسایی، جمع‌آوری، اکتساب و حفظ اطلاعاتی که می‌توانند به عنوان شواهد مورد استفاده قرار گیرند، تعریف نموده و به کار گیرد.
الف.۱۷: جوانب امنیت اطلاعات در مدیریت تداوم کسب و کار		
الف.۱,۱۷: تداوم امنیت اطلاعات		
هدف: تداوم امنیت اطلاعات باید در سیستم‌های مدیریت تداوم کسب و کار سازمان، لحاظ شود.		
الف.۱,۱,۱۷	طرح‌ریزی تداوم امنیت اطلاعات	کنترل: سازمان باید الزاماتش را برای امنیت اطلاعات و تداوم مدیریت امنیت اطلاعات در وضعیت‌های نامطلوب، به عنوان مثال هنگام بحران یا فاجعه، تعیین کند.
الف.۲,۱,۱۷	پیاده‌سازی تداوم امنیت اطلاعات	کنترل: به منظور حصول اطمینان از سطح الزامی تداوم برای امنیت اطلاعات در هنگام یک موقعیت نامطلوب، سازمان باید فرایندها، رویه‌ها و کنترل‌هایی را وضع، مدون، پیاده‌سازی و نگهداری کند.
الف.۳,۱,۱۷	بررسی، بازنگری و ارزیابی تداوم امنیت اطلاعات	کنترل: سازمان باید کنترل‌های تداوم امنیت اطلاعات را که وضع و پیاده‌سازی شده اند، در فواصل زمانی منظم بررسی کند تا اطمینان حاصل شود این کنترل‌ها در هنگام وضعیت‌های نامطلوب، معتبر و مؤثر هستند.
الف.۲,۱۷: جایگزین‌ها		
هدف: حصول اطمینان از دسترس‌پذیری امکانات پردازش اطلاعات		
الف.۱,۲,۱۷	دسترس‌پذیری امکانات پردازش اطلاعات	کنترل: امکانات پردازش اطلاعات باید با جایگزین‌های کافی جهت برآورده‌سازی الزامات دسترس‌پذیری، پیاده‌سازی شوند.
الف.۱۸: انطباق		
الف.۱,۱۸: انطباق با الزامات قانونی و قراردادی		
هدف: پرهیز از نقض تعهدات قانونی، حقوقی، مقرراتی یا قراردادی مرتبط با امنیت اطلاعات و هر الزام امنیتی		
الف.۱,۱,۱۸	شناسایی الزامات قانونی و قراردادی قابل اجرا	کنترل: تمامی الزامات قانونی، حقوقی، مقرراتی، قراردادی مرتبط و رویکرد سازمان نسبت به تحقق این الزامات، باید برای هر یک از سیستم‌های اطلاعاتی و سازمان، به وضوح شناسایی، مدون و به روز نگهداشته شوند.
الف.۲,۱,۱۸	حقوق مالکیت معنوی	کنترل: رویه‌های مناسب، به منظور حصول اطمینان از انطباق با الزامات قانونی،

		مقرراتی و قراردادی مرتبط با حقوق مالکیت معنوی و استفاده از محصولات نرم افزاری دارای حقوق مالکیت، باید پیاده‌سازی شوند.
الف.۳,۱,۱۸	حفاظت از سوابق	کنترل: سوابق باید مطابق با الزامات قانونی، مقرراتی، قراردادی و الزامات کسب و کار در برابر فقدان، تخریب، تحریف، دسترسی غیرمجاز و افشای غیرمجاز محافظت شوند.
الف.۴,۱,۱۸	حریم خصوصی و حفاظت از اطلاعات هویت شخصی	کنترل: در صورت قابلیت پیاده‌سازی حریم خصوصی و حفاظت از اطلاعات هویتی شخصی باید همانگونه که در قوانین و مقررات مرتبط الزام شده است، تضمین شود.
الف.۵,۱,۱۸	قواعد کنترل‌های رمزنگاری	کنترل: کنترل‌های رمزنگاری باید منطبق با تمامی توافق‌نامه‌ها، قوانین و مقررات مرتبط، به کار گرفته شوند.
الف.۲,۱۸: بازنگری‌های امنیت اطلاعات		
هدف: حصول اطمینان از اینکه امنیت اطلاعات، مطابق با خط‌مشی‌ها و رویه‌های سازمانی، پیاده‌سازی و اجرا می‌شوند.		
الف.۱,۲,۱۸	بازنگری مستقل امنیت اطلاعات	کنترل: رویکرد سازمان نسبت به مدیریت امنیت اطلاعات و پیاده‌سازی آن (به عنوان مثال اهداف کنترلی، کنترل‌ها، خط‌مشی‌ها، فرایندها و رویه‌های امنیت اطلاعات)، باید در فواصل زمانی طرح‌ریزی شده یا هنگامی که تغییرات مهمی رخ می‌دهد، به طور مستقل بازنگری شود.
الف.۲,۲,۱۸	انطباق با خط‌مشی‌ها و استانداردهای امنیتی	کنترل: مدیران باید انطباق پردازش اطلاعات و رویه‌ها را در حیطه مسئولیت‌شان، با خط‌مشی‌ها و استانداردهای امنیتی مناسب و دیگر الزامات امنیتی، به طور منظم بازنگری کنند.
الف.۳,۲,۱۸	بازنگری انطباق فنی	کنترل: سیستم‌های اطلاعاتی باید به منظور انطباق با خط‌مشی‌ها و استانداردهای امنیت اطلاعات سازمان، به طور منظم بازنگری شوند.

کتابنامه

۱- ISO/IEC 27002:2013، فناوری اطلاعات – فنون امنیتی – آیین‌کار کنترل‌های امنیت اطلاعات

۲- ISO/IEC 27003، فناوری اطلاعات – فنون امنیتی – راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات

۳- ISO/IEC 27004، فناوری اطلاعات – فنون امنیتی – مدیریت امنیت اطلاعات - سنجش

۴- ISO/IEC 27005، فناوری اطلاعات – فنون امنیتی – مدیریت مخاطرات امنیت اطلاعات

۵- ISO 31000:2009، مدیریت مخاطرات – اصول و راهنماها

۶- دستورالعمل‌های ISO/IEC، بخش ۱، مکمل‌های تلفیقی ISO – رویه‌های مختص ISO، ۲۰۱۲