ISO/IEC 27001:2013

INFORMATION SECURITY MANAGEMENT

مدیریت امنیت اطلاعات

فهرست

پیشگفتار

سازمان بین المللی استاندارد(ISO) و کمیسیون بین المللی الکتروتکنیک(IEC)، سیستمی تخصصی را جهت استانداردسازی در سطح دنیا ایجاد کرده اند.. نهادهای ملی عضو ISO یا IEC، توسط کمیته های فنی تدوین شده از سوی سازمان مربوطه شان، در تدوین استانداردهای بین المللی مشارکت می کنند و به زمینه های خاص فعالیتهای فنی می پردازند. کمیته های فنی ISO وIEC، در زمینه هایی با منافع مشترک، با همدیگر همکاری می کنند. سایر سازمان های بین المللی، 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 داده اند.

پیش نویس استانداردهای بین المللی، مطابق با قوانین مندرج در بخش ۲ دستورالعمل های ISO/IEC تهیه شده است.

وظیفه اصلی کمیته فنی مشترک، آماده سازی استانداردهای بین المللی است. پیش نویس استانداردهای بین المللی مورد تأیید کمیته فنی مشترک، برای رای گیری در اختیار نهادهای ملی قرار می گیرد.. انتشار به عنوان استاندارد بین المللی 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 IECمسئولیتی 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

۰-۱ کلیات

این استاندارد بین المللی، به منظور ارایه الزاماتی برای استقرار، پیاده سازی، نگه داری 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 پیاده سازی 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 می رود 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 دسترس پذیری اطلاعات محافظت میکند و به طرفهای ذینفع این اطمینان را میدهد که مخاطرات، به میزان کافی مدیریت می شوند.

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، سیستم های اطلاعاتی و کنترلها لحاظ میشود. انتظار می رود که پیاده سازی یک سیستم مدیریت امنیت اطلاعات، منطبق با نیازهای سازمان باشد.

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

ترتیب ارایه الزامات در این استاندارد بین المللی، بیان کننده اهمیت یا ترتیب پیاده سازی آنها نیست. موارد فهرست شده، به منظور ارجاع های بعدی ذکر شده شداند.

استاندارد ISO/IEC 27000، نمای کلی و واژگان سیستم های مدیریت امنیت اطلاعات را توصیف نموده و مرجع خانواده استاندارد سیستم مدیریت امنیت اطلاعات (شامل ISO/IEC 270042،ISO/IEC 27003 و ISO/IEC 27005) به همراه اصطلاحات و تعاریف مرتبط با آن است.

۰-۲ سازگاری با سایر استانداردهای سیستم مدیریت

این استاندارد بین المللی از ساختار سطح بالا، عناوین یکسان در بندهای فرعی، متن یکسان، اصطلاحات مشترک و تعاریف اصلی موجود در پیوست SL بخش 7 دستورالعمل های ISO/IEC، مکمل های تلفیقی ISO استفاده می کند و در نتیجه با سایر استانداردهای سیستم مدیریت که پیوست SL را پذیرفته اند، سازگار است.

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

فناوری اطلاعات – فنون امنیتی – سیستم های مدیریت امنیت اطلاعات – الزامات

۱– دامنه کاربرد

این استاندارد بین المللی، الزاماتی را برای استقرار، پیاده سازی، نگه داری و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات در چارچوب سازمان، مشخص میکند. این استاندارد بین المللی، همچنین شامل الزاماتی برای ارزیابی و برطرف سازی مخاطرات امنیت اطلاعات، متناسب با نیازهای سازمان است. الزامات تعیین شده در این استاندارد بین المللی، عمومی بوده و در تمام سازمان ها، 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 بین المللی 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 گرفته اند و در راستای کاربرد این سند، مراجعی که با ذکر تاریخ، ارجاع داده شده اند فقط همان ویرایش، و مراجعی که بدون ذکر تاریخ، ارجاع داده شده اند آخرین ویرایش سند اشاره شده (شامل همه اصلاحیه ها) مورد استناد است.

ISO/IEC 27000، فناوری اطلاعات – فنون امنیتی – سیستم های 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 می روند.

۴- زمینه سازمان

۴-۱ درک سازمان و زمینه آن

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

*نکته۱: تعیین این مسایل به استقرار چارچوب بیرونی و درونی سازمان که در بند ۵-۳ از استاندارد ISO 31000:2009 مطرح شده است، اشاره دارد.

۴-۲ درک 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 محدوده سیستم مدیریت امنیت اطلاعات

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

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

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

ب) الزامات اشاره شده در بند ۲.۴؛ و

ج) واسط ها و وابستگی های بین فعالیت های انجام شده توسط سازمان و فعالیت هایی که توسط سازمان های دیگر انجام می شوند.

محدوده 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 بین المللی، ایجاد، پیاده سازی و نگه داری کند و آن را به طور مستمر بهبود بخشد.

۵- رهبری

۵-۱ 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 خط مشی 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 شده اند.

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 می یابد.

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

ز) ترویج بهبود مستمر؛ و

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

۵-۲ خط مشی

مدیریت ارشد باید یک خط مشی امنیت اطلاعات ایجاد کند که:

الف) متناسب با هدف سازمان باشد.

ب) شامل اهداف امنیت اطلاعات باشد (به بند۶-۲ مراجعه شود) یا چارچوبی را برای تعیین اهداف امنیت اطلاعات ارایه دهد.

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

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

خط مشی 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.

۵-۳ نقش های سازمانی، مسئولیت ها و اختیارات

مدیریت ارشد باید اطمینان حاصل کند که مسئولیت ها و اختیارات برای نقش های مرتبط با امنیت اطلاعات، تعیین و ابلاغ شده اند.

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 بین المللی؛ 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

۶-۱ اقدامات جهت پرداختن به مخاطرات و فرصتها

۶-۱-۱ کلیات

هنگام طرح ریزی سیستم مدیریت امنیت اطلاعات، سازمان باید مسایل اشاره شده در بند ۴-۱ و الزامات اشاره شده در بند ۴-۲ 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 پیاده سازی این اقدامها در فرایندهای سیستم مدیریت امنیت اطلاعات سازمان؛ و

۲- ارزشیابی اثربخشی این اقدامات.

۶-۱-۲ 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 نگه داری کند که شامل موارد زیر باشد:

۱- معیارهای پذیرش مخاطرات؛ و

۲- معیارهایی برای انجام ارزیابی مخاطرات امنیت اطلاعات.

ب) اطمینان دهد که تکرار ارزیابی های مخاطرات امنیت اطلاعات، نتایج سازگار، معتبر و قیاس پذیر تولید می کنند.

ج) مخاطرات امنیت اطلاعات را شناسایی کند.

۱- به کارگیری فرایند ارزیابی مخاطرات امنیت اطلاعات برای شناسایی مخاطرات مربوط به فقدان محرمانگی، صحت و دسترس پذیری اطلاعات در محدوده سیستم مدیریت امنیت اطلاعات؛ و

۲- شناسایی مالکان مخاطره.

د) مخاطرات امنیت اطلاعات را تحلیل کند.

۱-ارزیابی پیامدهای بالقوه که ممکن است در صورت تحقق مخاطرات شناسایی شده در بند پ ۶-۱-۲ رخ دهد.

۲- ارزیابی واقع بینانه فرصت وقوع مخاطرات شناسایی شده در بند پ ۶-۱-۲

۳- تعیین سطوح مخاطرات.

ه) مخاطرات امنیت اطلاعات را ارزشیابی کند:

۱- مقایسه نتایج تحلیل مخاطرات با معیارهای مخاطرات ایجاد شده در بند الف ۶-۱-۲

۲- اولویت بندی مخاطرات تحلیل شده برای برطرف سازی مخاطرات.

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

۶-۱-۳ برطرف سازی مخاطرات امنیت اطلاعات

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

الف) با درنظر گرفتن نتایج ارزیابی مخاطرات، گزینه های مناسب جهت برطرف سازی مخاطرات امنیت اطلاعات را انتخاب نماید.

ب) تمامی کنترل های ضروری به منظور پیاده سازی گزینه(های) انتخابی برطرف سازی مخاطرات امنیت اطلاعات را تعیین کند.

*نکته: سازمان ها میتوانند در صورت لزوم، کنترل هایی طراحی کنند یا آنها را از هر منبع دیگری شناسایی کنند.

ج) کنترل های تعیین شده در بالا (بند ب ۶-۱-۳) را با کنترل های موجود در پیوست الف، مقایسه کرده و بررسی کند که هیچ یک از کنترل های ضروری حذف نشده است.

یادآوری ۱: پیوست الف شامل فهرست جامعی از اهداف کنترلی و کنترلها است. استفاده کنندگان از این استاندارد بین المللی برای حصول اطمینان از اینکه هیچ یک از کنترل های ضروری نادیده گرفته نشده است، به پیوست الف ارجاع داده می شوند.

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

د) یک بیانیه کاربردپذیری که شامل کنترل های ضروری (مراجعه به بند ب و پ ۶-۱-۳) و دلیل استفاده از آنها بدون درنظر گرفتن اینکه پیاده سازی شده یا نشده اند و توجیه کنارگذاری کنترل های پیوست الف باشد، ایجاد نماید.

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

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

سازمان باید اطلاعاتی مستند درباره فرایند برطرف سازی مخاطرات امنیت اطلاعات، نگه داری کند.

*یادآوری: فرایند ارزیابی و برطرف سازی مخاطرات امنیت اطلاعات در این استاندارد بین المللی، با اصول و رهنمودهای کلی / عمومی موجود در ISO 31000 مطابقت دارد.

۶-۲ 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 خط مشی امنیت اطلاعات، سازگار باشند.

ب) قابل اندازه گیری باشند (در صورت عملی بودن)؛

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

د) ابلاغ شوند؛ و

ه)در صورت نیاز، به روزرسانی شوند.

سازمان باید اطلاعاتی مستند را درباره اهداف امنیت اطلاعات، نگه داری 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

۷-۱ منابع

سازمان باید منابع مورد نیاز به منظور استقرار، پیاده سازی، نگه داری و بهبود مستمر سیستم مدیریت امنیت اطلاعات را تعیین و فراهم کند.

۷-۲ صلاحیت

سازمان باید:

الف) صلاحیت های مورد نیاز افرادی که تحت کنترل سازمان کار می کنند 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، نگه داری کند.

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

۷-۳ آگاه سازی

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

الف) خط مشی 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.

۷-۴ 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 زمینه ای 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.

۷-۵ اطلاعات مستند

۷-۵-۱ کلیات

سیستم مدیریت امنیت اطلاعات سازمان باید شامل این موارد باشد:

الف) اطلاعات مستند مورد نیاز این استاندارد بین المللی؛ و

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

یادآوری: گستره مستندسازی سیستم مدیریت امنیت اطلاعات می تواند به دلایل زیر برای هر سازمان متفاوت باشد:

الف) اندازه سازمان و نوع فعالیتها، فرایندها، محصولات و خدمات آن؛

ب) پیچیدگی فرایندها و تعاملات آنها؛ و

ج) صلاحیت افراد.

۷-۵-۲ 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 (مثلا کاغذی، الکترونیکی)؛ و

ج) بازنگری و تصویب جهت سازگاری و کفایت.

۷-۵-۳ کنترل اطلاعات مستند

اطلاعات مستند مورد نیاز سیستم مدیریت امنیت اطلاعات و این استاندارد بین المللی 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 می شوند (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) ذخیره سازی و محافظت، شامل حفظ خوانایی؛

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

و) نگه داشتن 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.

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

۸-۱ طرحریزی و کنترل عملیات

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

سازمان باید اطلاعات مستند تا حدی ضروری را برای حصول اطمینان از اینکه فرایندها مطابق با طرحها پیشروی داشته اند ،نگه داری 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 می شوند.

۸-۲ ارزیابی مخاطرات امنیت اطلاعات

سازمان باید ارزیابی مخاطرات امنیت اطلاعات را در بازه های زمانی طرحریزی شده یا هنگام وقوع تغییرات مهم یا تغییرات پیشنهاد شده، با درنظر گرفتن معیار ایجاد شده در بند-۲-۱۶ الف، انجام دهد.

سازمان باید اطلاعاتی مستند را درباره نتایج ارزیابی های مخاطرات امنیت اطلاعات، نگه داری کند.

۸-۳ برطرف سازی مخاطرات امنیت اطلاعات

سازمان باید طرح برطرف سازی مخاطرات امنیت اطلاعات را پیاده سازی کند.

سازمان باید اطلاعاتی مستند را درباره نتایج برطرف سازی مخاطرات امنیت اطلاعات، نگه داری کند.

۹- ارزشیابی عملکرد

۹-۱ پایش، اندازه گیری، 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 اندازه گیری نیاز دارند، از جمله فرایندها و کنترل های امنیت اطلاعات؛

ب) در صورت قابلیت اعمال، روش هایی برای پایش، اندازه گیری، تحلیل و ارزشیابی، به منظور حصول اطمینان از معتبر بودن نتایج؛

یادآوری- روش های انتخابی باید نتایج قابل قیاس و تکرارپذیر تولید کنند تا معتبر شناخته شوند.

ج)چه زمانی باید پایش و اندازه گیری انجام شود.

د)چه کسی باید پایش و اندازه گیری را انجام دهد.

ه) چه زمانی نتایج حاصل از پایش و اندازه گیری 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 اندازه گیری نتایج، نگه داری کند.

۹-۲ ممیزی داخی

سازمان باید ممیزی های داخلی را در فاصله های 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 بین المللی؛

ب) به طور اثربخش، پیاده سازی و نگه داری میشود.

سازمان باید:

پ) برنامه(های) ممیزی شامل دفعات تکرار، روش ها، مسئولیت ها، الزامات طرحریزی و گزارش دهی را طرحریزی، مستقر ،پیاده سازی و نگه داری کند. برنامه(های) ممیزی باید اهمیت فرایندهای مورد نظر و نتایج ممیزی های قبلی را درنظر بگیرند.

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

ه)در انتخاب ممیزان و انجام ممیزی ها، از واقع بینی و بی طرفی فرایند ممیزی اطمینان حاصل نماید.

و) اطمینان حاصل کند که نتایج ممیزی ها به مدیریت مربوطه گزارش داده می شوند؛ و

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

۹-۳ بازنگری مدیریت

مدیریت ارشد باید سیستم مدیریت امنیت اطلاعات سازمان را در فاصله های 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 بازنگری های 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 انطباق ها و اقدام های اصلاحی؛

۲- نتایج پایش و اندازه گیری؛

۳-نتایج ممیزی؛ و

۴- تحقق اهداف امنیت اطلاعات.

د) بازخورد از طرفهای ذینفع؛

ه) نتایج ارزیابی مخاطرات و وضعیت طرح برطرف سازی مخاطرات؛ و

و) فرصت ها برای بهبود مستمر.

خروجی های بازنگری مدیریت باید دربرگیرنده تصمیمات مربوط به فرصت های بهبود مستمر و هرگونه نیاز به تغییر در سیستم مدیریت امنیت اطلاعات باشد.

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

۱۰- بهبود

۱۰-۱ 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 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 انطباق های مشابه یا احتمال وقوع آنها.

ج) اقدام های مورد نیاز را پیاده سازی کند.

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

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

اقدام های اصلاحی باید متناسب با اثرات عدم انطباق های مشاهده شده باشند.

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

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

ز) نتایج هر یک از اقدام های اصلاحی.

۱۰-۲ بهبود مستمر

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

پیوست الف

(الزامی)

کنترل ها و اهداف کنترلی مرجع

اهداف کنترلی و کنترل های فهرست شده در جدول الف.۷، به طور مستقیم از بندهای ۵ تا ۱۸ استاندارد ISO/IEC 27002:2013 و منطبق با آنها برگرفته شده اند و در چارچوب بند ۶-۱-۳ مورد استفاده قرار خواهند گرفت.

جدول الف : اهداف کنترلی و کنترل ها

الف ۵ خط مشی های امنیت اطلاعات		
الف ۵-۱: هدایت مدیریت برای امنیت اطلاعات		
هدف: تأمین هدایت و پشتیبانی مدیریت از تطابق امنیت اطلاعات، مطابق با الزامات کسب و کار و قوانین و آیین نامه های مرتبط		
الف۵-۱-۱	خط مشی های امنیت اطلاعات	کنترل: مجموعه ای از خط مشی های امنیت اطلاعات، باید تعریف و توسط مدیریت تصویب شود، منتشر شده و به اطلاع کارکنان و طرفهای مرتبط بیرونی برسد.
الف۵-۱-۲	بازنگری خط مشی های امنیت اطلاعات	کنترل: خط مشی های 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 پیاده سازی و اجرای امنیت اطلاعات در درون سازمان		
الف۶-۱-۱	نقش ها و مسئولیت های امنیت اطلاعات	کنترل: کلیه مسئولیت های امنیت اطلاعات، باید تعریف و محول شوند.
الف۶-۱-۲	تفکیک وظایف	کنترل: به منظور کاهش فرصت های دستکاری غیرمجاز یا غیرعمد، یا سوءاستفاده از دارایی های سازمان، باید وظایف و حدود مسئولیت های مغایر، تفکیک شوند.
الف۶-۱-۳	ارتباط با مراجع معتبر	کنترل: ارتباطات مقتضی با مراجع معتبر مرتبط باید حفظ شود.
الف۶-۱-۴	ارتباط با گروه های ذینفع ویژه	کنترل: ارتباطات مقتضی با گروههای ذینفع ویژه یا سایر انجمن های امنیتی متخصص و انجمن های حرفه ای باید حفظ شود.

الف۶-۱-۵	امنیت اطلاعات در مدیریت پروژه	کنترل: امنیت اطلاعات باید در مدیریت پروژه، صرفنظر از نوع پروژه، لحاظ شود.
الف ۶-۲ دستگاه های قابل حمل و دورکاری		
هدف: حصول اطمینان از امنیت دورکاری و استفاده از دستگاه های قابل حمل		
الف۶-۲-۱	خط مشی دستگاه های قابل حمل	کنترل: یک خط مشی و اقدامات امنیتی پشتیبان، به منظور مدیریت مخاطرات ایجاد شده به دلیل استفاده از دستگاه های قابل حمل، باید اتخاذ گردد.
الف۶-۲-۲	دورکاری	کنترل: یک خط مشی و اقدامات امنیتی پشتیبان، به منظور حفاظت از اطلاعات قابل
الف ۷ امنیت منابع انسانی		
الف ۷-۱ پیش از اشتغال		
هدف : حصول اطمینان از اینکه کارکنان و پیمانکاران از مسئولیتهای امنیت اطلاعات خود، آگاه بوده و آنها را به انجام میرسانند.		
الف ۷-۱-۱	گزینش	کنترل: مدیریت باید تمامی کارکنان و پیمانکاران را به کارگیری امنیت اطلاعات ،مطابق با خط مشی ها و رویه های ایجاد شده سازمان، الزام نماید.
الف ۷-۱-۲	ضوابط و شرایط استخدام	کنترل: توافق های قراردادی با کارکنان و پیمانکاران باید بیانگر مسئولیتهای ایشان و سازمان، در قبال امنیت اطلاعات باشد.
الف ۷-۲ در حین خدمت		
هدف: حصول اطمینان از اینکه کارکنان و پیمانکاران از مسئولیت های امنیت اطلاعات خود، آگاه بوده و آنها را به انجام میرسانند.		
الف ۷-۲-۱	مسئولیت های مدیریت	کنترل: مدیریت باید تمامی کارکنان و پیمانکاران را به کارگیری امنیت اطلاعات، مطابق با خط مشی ها و رویه های ایجاد شده سازمان، الزام نماید.
الف ۷-۲-۲	آگاه سازی، تحصیل و آموزش امنیت اطلاعات	کنترل: تمامی کارکنان سازمان، و در صورت لزوم پیمانکاران، باید به صورت مناسب، در خصوص خط مشی ها و رویه های سازمان، آگاه سازی، تحصیل و آموزش مناسب ببینند و به طور منظم به روز شوند، به طوری که به کارکرد شغلی ایشان مرتبط باشد.
الف ۷-۲-۳	فرایند انضباطی	کنترل: باید برای اقدام در برابر کارکنانی که مرتکب نقض امنیت اطلاعات شده اند یک فرایند انضباطی رسمی و ابلاغ شده، وجود داشته باشد.
الف ۷-۳ خاتمه و تغییر اشتغال		
هدف: محافظت از منافع سازمان، به عنوان بخشی از فرایند تغییر یا خاتمه اشتغال		
الف ۷-۳-۱	مسئولیت های خاتمه اشتغال یا تغییر شغل	کنترل: مسئولیت ها و وظایف امنیت اطلاعات که پس از خاتمه اشتغال یا تغییر شغل، معتبر باقی می مانند باید تعریف شده، به کارکنان یا پیمانکاران ابلاغ و اجبار شوند.

الف ۸: مدیریت دارایی		
الف ۸-۱ مسئولیت دارایی ها		
هدف: شناسایی دارایی های سازمانی و تعریف مسئولیت های حفاظت مناسب		
الف ۸-۱-۱	فهرست دارایی ها	کنترل: دارایی های مرتبط با اطلاعات و امکانات پردازش اطلاعات باید شناسایی شده و فهرستی از این دارایی ها تنظیم و نگهداری شود.
الف ۸-۱-۲	مالکیت دارایی ها	کنترل: دارایی های نگهداری شده در فهرست باید دارای مالک باشند.
الف ۸-۱-۳	استفاده قابل قبول از دارایی ها	کنترل: قوانینی برای استفاده قابل قبول از اطلاعات و دارایی های مرتبط با اطلاعات و امکانات پردازش اطلاعات، باید شناسایی، مدون و پیاده سازی شوند.
الف ۸-۱-۴	بازگرداندن دارایی ها	کنترل: تمامی کارکنان و کاربران شخص ثالث باید کلیه دارایی های سازمانی را که در اختیار دارند، به محض خاتمه اشتغال، قرارداد یا توافقنامه، به سازمان بازگردانند.
الف ۸-۲ طبقه بندی اطلاعات		
هدف: حصول اطمینان از اینکه اطلاعات، با توجه به اهمیت آن برای سازمان، به سطح حفاظتی مناسب رسیده است.		
الف ۸-۲-۱	طبقه بندی اطلاعات	کنترل: اطلاعات باید با توجه به الزامات قانونی، ارزش، بحرانی بودن و حساس بودن در برابر افشای غیر مجاز یا تغییرات طبقه بندی شوند.
الف ۸-۲-۲	علامت گذاری اطلاعات	کنترل: باید مجموعه مناسبی از رویه هایی برای برچسب گذاری اطلاعات، با توجه به الگوی طبقه بندی اطلاعات پذیرفته شده توسط سازمان، ایجاد و پیاده سازی شود.
الف ۸-۲-۳	اداره کردن دارایی	کنترل: باید رویه هایی برای اداره کردن دارایی ها، با توجه به الگوی طبقه بندی اطلاعات پذیرفته شده توسط سازمان، ایجاد و پیاده سازی شود.
الف ۸-۳ اداره کردن رسانه های ذخیره سازی		
هدف: پیشگیری از افشا، دستکاری، حذف یا تخریب غیرمجاز اطلاعات ذخیره شده در رسانه ها		
الف ۸-۳-۱	مدیریت رسانه های جدا شدنی	کنترل: باید رویه هایی برای مدیریت رسانه های جدا شدنی، با توجه به الگوی طبقه بندی پذیرفته شده توسط سازمان، ایجاد و پیاده سازی شود.
الف ۸-۳-۲	امحاء رسانه	کنترل:رسانه ها باید زمانی که دیگر مورد نیاز نیستند، به صورت امن و با استفاده از رویه هایی رسمی، امحا شوند.
الف ۸-۳-۳	انتقال رسانه فیزیکی	کنترل: رسانه های 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	خط مشی کنترل دسترسی	کنترل: باید خط مشی کنترل دسترسی، بر مبنای الزامات کسب و کار و امنیت اطلاعات، ایجاد، مدون و بازنگری شود.
الف ۹-۱-۲	دسترسی به شبکه و خدمات 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 سیستم ها و سرویس ها		
الف ۹-۲-۱	ثبت و حذف کاربر	کنترل: باید فرایندی رسمی برای ثبت و حذف کاربر، به منظور ایجاد امکان اعطای حقوق دسترسی، پیاده سازی 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 سیستم ها و سرویس ها، پیاده سازی شود.
الف ۹-۲-۳	مدیریت حق دسترسی ویژه	کنترل: تخصیص و به کارگیری حق دسترسی ویژه، باید محدود و کنترل شود.
الف ۹-۲-۴	مدیریت اطلاعات محرمانه احراز هویت کاربران	کنترل: تخصیص اطلاعات محرمانه احراز هویت، باید از طریق یک فرایند رسمی مدیریتی، کنترل شود.
الف ۹-۲-۵	بازنگری	کنترل: مالکان دارایی ها باید حقوق دسترسی کاربران را در فواصل زمانی منظم بازنگری کنند.
الف ۹-۲-۶	حذف	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 مسئولیت های کاربر		
هدف: پاسخگو بودن کاربران در برابر حفاظت از اطلاعات اصالت سنجی شان		
الف ۹-۳-۱	استفاده از اطلاعات اصالت سنجی	کاربران باید به تبعیت از شیوه های سازمان در استفاده از اطلاعات محرمانه اصالت سنجی ملزم شوند.
الف ۹-۴ کنترل دسترسی به برنامه های کاربردی و سامانه ها		
پیشگیری از دسترسی غیرمجاز به سامانه ها و برنامه های کاربردی		
الف ۹-۴-۱	محدود سازی دسترسی به اطلاعات	کنترل: مطابق با خط مشی کنترل دسترسی، باید دسترسی به اطلاعات و کارکردهای سامانه کاربردی، محدود شود.

الف ۹-۴-۲	روش های اجرایی ورود امن	کنترل: در مواردی که خط مشی کنترل دسترسی الزام کرده است، دسترسی به سامانه ها باید از طریق یک روش اجرایی ورود امن به سامانه کنترل شود.
الف ۹-۴-۳	سیستم مدیریت کلمات عبور	کنترل: سیستم های مدیریت کلمات عبور، باید تعاملی بوده و باید کیفیت کلمات عبور را تضمین کند.
الف ۹-۴-۴	استفاده از برنامه های کمکی	استفاده از برنامه های کمکی سامانه که ممکن است دارای قابلیت ابطال کنترل های سامانه و برنامه کاربردی باشد؛ باید محدود و به شدت کنترل شود.
الف ۹-۴-۵	کنترل دسترسی به کد منبع برنامه ها	دسترسی به کد منبع برنامه باید محدود شود.
الف ۱۰ رمزنگاری		
الف ۱۰-۱ کنترل های رمزنگاری		
الف ۱۰-۱-۱	خط مشی استفاده از کنترل های رمزنگاری	کنترل: باید خط مشی استفاده از کنترل های رمزنگاری، برای حفاظت از اطلاعات، ایجاد و پیاده سازی شود.
الف ۱۰-۱-۲	مدیریت کلید	کنترل: خط مشی استفاده، حفاظت و طول عمر کلیدهای رمزنگاری، باید ایجاد و در کل چرخه حیات آنها پیاده سازی شود.
الف ۱۱ امنیت فیزیکی و محیطی		
الف ۱۱-۱ نواحی امن		
هدف: جلوگیری از دسترسی فیزیکی غیرمجاز، خسارت و مداخله در اطلاعات و امکانات پردازش اطلاعات سازمان		
الف ۱۱-۱-۱	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 ۱۱-۱-۲	کنترل های ورودی فیزیکی	کنترل: نواحی امن، به منظور حصول اطمینان از اینکه فقط کارکنان مجاز، اجازه دسترسی دارند، باید توسط کنترل های ورودی مناسب، حفاظت شوند.
الف ۱۱-۱-۳	امن سازی دفاتر، اتاق ها و امکانات	کنترل: امنیت فیزیکی برای دفاتر، اتاق ها و امکانات، باید طراحی شده و به کار گرفته شود.
الف ۱۱-۱-۴	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 ۱۱-۱-۵	کار در نواحی امن	کنترل: رویه هایی برای کار در نواحی امن، باید طراحی شده و به کار گرفته شود.

الف ۱۱-۱-۶	نواحی تحویل و بارگیری	کنترل۱: نقاط دسترسی مانند نواحی تحویل و بارگیری و سایر نقاطی که افراد متفرقه ممکن است وارد محوطه ها شوند، باید تحت کنترل قرار گیرند، و در صورت امکان، برای جلوگیری از دسترسی غیرمجاز، از امکانات پردازش اطلاعات، مجزا شوند.
الف ۱۱-۲ تجهیزات		
هدف: جلوگیری از فقدان، آسیب، سرقت یا به خطر افتادن دارایی ها و ایجاد وقفه در فعالیت های سازمان		
الف ۱۱-۲-۱	استقرار و حفاظت از تجهیزات	کنترل: تجهیزات باید (در محل مناسب) مستقر و محافظت شوند تا مخاطرات ناشی از تهدیدها و خطرات محیطی و فرصت های دسترسی غیرمجاز، کاهش یابند.
الف ۱۱-۲-۲	امکانات پشتیبانی	کنترل: تجهیزات باید در برابر خرابی برق و سایر اختلالات ناشی از خرابی امکانات پشتیبانی، محافظت شوند.
الف ۱۱-۲-۳	امنیت کابل کشی	کنترل) کابل کشی های 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 ۱۱-۲-۴	نگهداری تجهیزات	کنترل) تجهیزات باید به منظور حصول اطمینان از تداوم دسترس پذیری و صحت شان، به درستی نگهداری شوند.
الف ۱۱-۲-۵	خروج دارایی ها	کنترل) تجهیزات، اطلاعات یا نرم افزار، نباید بدون مجوز قبلی از محل خارج شوند.
الف ۱۱-۲-۶	امنیت تجهیزات و دارایی های خارج از ابنیه	کنترل) برای دارایی های خارج از ابنیه، باید با توجه به مخاطرات مختلف ناشی از انجام کار در خارج از بناهای سازمان، امنیت برقرار شود.
الف ۱۱-۲-۷	امحا یا استفاده مجدد از تجهیزات به صورت امن	کنترل) تمام اجزای تجهیزاتی که دارای رسانه ذخیره سازی 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 شده اند، بررسی شوند.
الف ۱۱-۲-۸	تجهیزات بدون مراقبت کاربر	کنترل) کاربران باید اطمینان حاصل کنند که تجهیزات بدون مراقبت، حفاظت مناسبی دارند.
الف ۱۱-۲-۹	خط مشی میز پاک و صفحه پاک	کنترل) خط مشی میز پاک برای اوراق و رسانه های ذخیره سازی جداشدنی، و خط مشی صفحه پاک برای امکانات پردازش اطلاعات، باید اتخاذ شود.
الف ۱۲ امنیت اطلاعات		
الف ۱۲-۱ مسئولیت ها و روش های اجرایی عملیاتی		
هدف: حصول اطمینان از کارکرد صحیح و امن امکانات پردازش اطلاعات		
الف ۱۲-۱-۱	رویه های عملیاتی مدون	کنترل) رویه های عملیاتی باید مدون شوند و در دسترس همه کاربرانی که به آنها نیاز دارند، قرار گیرند.

الف ۱۲-۱-۲	مدیریت تغییر	کنترل: تغییرات در سازمان، فرایندهای کسب و کار، امکانات و سیستم های پردازش اطلاعات که بر امنیت اطلاعات تأثیرگذار هستند، باید کنترل شوند.
الف ۱۲-۱-۳	مدیریت ظرفیت	کنترل: استفاده از منابع، باید پایش و تنظیم شده و پیش بینی ظرفیت مورد نیاز آینده جهت حصول اطمینان از کارایی الزامات سیستم، انجام شود.
الف ۱۲-۱-۴	جداسازی محیط های توسعه ،آزمایش و عملیاتی	کنترل: محیط های توسعه، آزمایش و عملیاتی، باید به منظور کاهش مخاطرات ناشی از دسترسی یا تغییر غیرمجاز در محیط عملیاتی، از یکدیگر جدا شوند.
الف ۱۲-۲ حفاظت در برابر بدافزار		
هدف: حصول اطمینان از محافظت از اطلاعات و تسهیلات پردازش اطلاعات در برابر بد افزار		
الف-۱۲-۲-۱	کنترل هایی در برابر بد افزار	کنترل: کنترل های لازم برای تشخیص، پیشگیری و ترمیم به منظور محافظت در برابر بدافزار، همراه با آگاه سازی مناسب کاربر باید پیاده سازی شوند.
الف ۱۲-۳ نسخه های پشتیبان		
هدف: محافظت در برابر از دست دادن داده ها		
الف ۱۲-۳-۱	پشتیبان گیری از اطلاعات	کنترل) نسخه های پشتیبان از اطلاعات، نرم افزار و تصاویر سیستم، باید با توجه به خط مشی مورد توافق پشتیبان گیری، تهیه و به صورت منظم آزمایش شوند.
الف ۱۲-۴ واقعه نگاری و پایش		
هدف: ثبت رویدادها و ایجاد شواهد		
الف ۱۲-۴-۱	واقعه نگاری رویداد	کنترل) واقعه نگاری رویدادها شامل ثبت فعالیت های کاربر، استثناءها، خطاها و رویدادهای امنیت اطلاعات، باید ایجاد، نگهداری و به صورت منظم بازنگری شوند.
الف ۱۲-۴-۲	حفاظت از اطلاعات ثبت شده رویدادها	کنترل) امکانات واقعه نگاری رویداد و اطلاعات ثبت شده، باید در برابر دستکاری و دسترسی غیرمجاز حفاظت شوند.
الف ۱۲-۴-۳	ثبت رویدادهای مدیر و اپراتور سیستم	کنترل) فعالیت های مدیر سیستم و اپراتور سیستم باید واقعه نگاری شوند و رویدادهای ثبت شده باید محافظت و به صورت منظم، بازنگری شوند.
الف ۱۲-۴-۴	همزمان سازی ساعتها	کنترل) ساعت های تمامی سیستم های پردازش اطلاعات مرتبط در درون یک سازمان یا دامنه اطلاعاتی، باید با یک منبع زمانی مرجع واحد، همزمان شوند.
الف ۱۲-۵ کنترل نرم افزارهای عملیاتی		
هدف: حصول اطمینان از صحت سیستم های عملیاتی		

الف ۱۲-۵-۱	نصب نرم افزار بر روی سیستم های عملیاتی	کنترل) رویه هایی برای کنترل نصب نرم افزار بر روی سیستم های عملیاتی باید پیاده سازی شوند.
الف ۱۲-۶ مدیریت آسیب پذیری فنی		
هدف: جلوگیری از سو استفاده از آسیب پذیری های فنی		
الف ۱۲-۶-۱	مدیریت آسیب پذیری های فنی	کنترل) اطلاعات در خصوص آسیب پذیری های فنی سیستم های اطلاعاتی مورد استفاده، باید به موقع کسب شود، قرارگیری سازمان در معرض چنین آسیب پذیری هایی ارزیابی شده و اقدامات مناسبی برای مقابله با مخاطرات مربوطه انجام شود.
الف ۱۲-۶-۲	محدودیت هایی برای نصب نرم افزار	کنترل) برای کنترل نصب نرم افزار توسط کاربران، باید قوانینی ایجاد و پیاده سازی شود.
الف.۱۲-۷ ملاحظات ممیزی سیستم های اطلاعاتی		
هدف: به حداقل رساندن تأثیر فعالیت های ممیزی بر سیستم های عملیاتی		
	کنترل های ممیزی سیستم های اطلاعاتی	کنترل: الزامات و فعالیت های ممیزی مرتبط با بررسی سیستم های عملیاتی، باید به دقت طرحریزی شده و مورد توافق قرار گیرند تا ایجاد وقفه در فرایندهای کسب و کار به حداقل برسد.
الف۱۳ امنیت ارتباطات		
الف.۱۳-۱ مدیریت امنیت شبکه		
هدف: حصول اطمینان از حفاظت اطلاعات در شبکهها و امکانات پردازش اطلاعات پشتیبان آنها		
الف ۱۳-۱-۱	کنترل های شبکه	کنترل: شبکه ها باید مدیریت و کنترل شوند تا از اطلاعات درون سیستم ها و برنامه ها محافظت شود.
الف ۱۳-۱-۲	امنیت سرویس های شبکه	کنترل: سازوکارهای امنیتی، سطوح خدمات و الزامات مدیریتی تمامی سرویس های شبکه، باید شناسایی شده و چه این سرویس ها به صورت درون سازمانی تأمین و چه برونسپاری شده اند، در توافقنامه های سرویس های شبکه لحاظ شوند.
الف ۱۳-۱-۳	تفکیک شبکه ها	کنترل: گروه های سرویس های اطلاعاتی، کاربران و سیستم های اطلاعاتی، باید در شبکه ها تفکیک شوند.
الف ۱۳-۲ انتقال اطلاعات		
هدف: حفظ امنیت اطلاعات منتقل شده درون سازمانی، با هر یک از موجودیت های بیرونی		

کنترل: برای حفاظت از انتقال اطلاعات به واسطه استفاده از تمامی انواع امکانات ارتباطی، باید خط مشی ها، رویه ها و کنترل های رسمی انتقال، تعیین شوند.		
الف.۱۳-۲-۱	خط مشی ها و رویه های انتقال اطلاعات	کنترل: برای حفاظت از انتقال اطلاعات به واسطه استفاده از تمامی انواع امکانات ارتباطی، باید خط مشی ها، رویه ها و کنترل های رسمی انتقال، تعیین شوند.
الف.۱۳-۲-۲	توافقنامه های انتقال اطلاعات	کنترل: توافقنامه ها باید انتقال اطلاعات کسب و کار را به صورت امن، مابین سازمان و طرف های بیرونی، لحاظ کنند.
الف ۱۳-۲-۳	پیام رسانی الکترونیکی	کنترل: اطلاعات درگیر در پیام رسانی الکترونیکی، باید به صورت مناسبی حفاظت شوند.
الف ۱۳-۲-۴	توافقنامه های محرمانگی یا عدم افشا	کنترل: الزامات توافقنامه های 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.۱۴-۱ الزامات امنیتی سیستم های اطلاعاتی		
هدف: حصول اطمینان از اینکه امنیت اطلاعات، یک جزء جدایی ناپذیر از سیستم های اطلاعاتی در طول کل چرخه حیات است. این موضوع شامل الزاماتی برای سیستم های اطلاعاتی که تأمین کننده سرویس هایی بر روی شبکه های عمومی هستند نیز میشود.		
الف.۱۴-۱-۱	تحلیل و تعیین الزامات امنیت اطلاعات	کنترل: الزامات مربوط به امنیت اطلاعات باید در الزامات سیستم های اطلاعاتی جدید یا گسترش سیستم های اطلاعاتی موجود لحاظ شوند.
الف.۱۴-۱-۲	ایمن سازی سرویس های برنامه بر روی شبکه های عمومی	کنترل:۱ اطلاعات درگیر در سرویس های برنامه که بر روی شبکه های عمومی منتقل میشوند باید در برابر فعالیت های متقلبانه، اختلافات قرارداد، دستکاری و افشای غیرمجاز محافظت شوند.
الف ۱۴-۱-۳	حفاظت از تراکنش های خدمات کاربری	کنترل: اطلاعات درگیر در تراکنش های خدمات کاربردی، به منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه، تغییر غیرمجاز پیام، افشای غیرمجاز و تکرار یا پاسخدهی غیرمجاز به پیام باید محافظت شوند.
الف ۱۴-۲ امنیت در فرایندهای توسعه و پشتیبانی		
هدف: حصول اطمینان از اینکه امنیت اطلاعات، در درون چرخه حیات سیستم های اطلاعاتی، طراحی و پیاده سازی شده است.		
الف ۱۴-۲-۱	خط مشی توسعه امن	کنترل: برای توسعه نرم افزار و سیستم ها، باید قوانینی وضع شده و در توسعه های درون سازمان به کار گرفته شود.
الف ۱۴-۲-۲	رویه های کنترل تغییر سیستم	کنترل: تغییرات بر روی سیستم ها در طول چرخه حیات توسعه باید با استفاده از رویه های رسمی کنترل تغییر، کنترل شوند.

الف ۱۴-۲-۳	بازنگری فنی برنامه ها پس از تغییرات بسترهای عملیاتی	کنترل: هنگام تغییر بسترهای عملیاتی، برنامه های حیاتی کسب و کار باید بازنگری و آزمایش شوند تا از عدم وجود تأثیر سوء بر عملیات یا امنیت سازمانی، اطمینان حاصل شود.
الف ۱۴-۲-۴	محدودسازی در اعمال تغییر	کنترل: باید از دستکاری در بسته های نرم افزاری اجتناب شده، محدود به تغییرات ضروری باشد، و تمامی تغییرات باید به شدت کنترل شوند.
الف ۱۴-۲-۵	اصول مهندسی نرم افزار امن	کنترل: باید اصولی برای مهندسی سیستم های امن استقرار یابد، مستند شده، نگه داری شده و برای هر گونه پیاده سازی سامانه اطلاعاتی، به کارگیری شود.
الف ۱۴-۲-۶	محیط توسعه امن	کنترل: سازمان ها باید محیط های توسعه امن را جهت توسعه و یکپارچه سازی سامانه که کل چرخه توسعه را در بر می گیرد، مستقر و به طور مناسب حفاظت کنند.
الف ۱۴-۲-۷	توسعه برون سپاری شده	کنترل: سازمان باید فعالیت توسعه سامانه به صورت برون سپاری شده را، نظارت و پایش کند.
الف ۱۴-۲-۸	آزمون امنیت سامانه	کنترل: باید آزمون کارکرد امنیتی، در طول توسعه انجام شود.
الف ۱۴-۲-۹	آزمون پذیرش سامانه ها	کنترل: برنامه های آزمون پذیرش و معیارهای مرتبط برای سامانه های اطلاعاتی جدید، ارتقا ها و ویرایش های جدید، باید ایجاد شود.
الف ۱۴-۳ داده های آزمون		
حصول اطمینان از محافظت داده مورد استفاده برای آزمایش		
الف ۱۴-۳-۱	حفاظت از داده های آزمایشی	کنترل: داده های آزمایشی، باید به دقت انتخاب شده، محافظت و کنترل شوند.
الف ۱۵ روابط تامین کنندگان		
الف ۱۵-۱ امنیت اطلاعات در روابط تامین کنندگان		
هدف: حصول اطمینان از حفاظت دارایی های سازمان که در دسترس تامین کنندگان است.		
الف ۱۵-۱-۱	خط مشی امنیت اطلاعات برای روابط تامین کنندگان	کنترل: الزامات امنیت اطلاعات برای کاهش مخاطرات مربوط به دسترسی تامین کنندگان به دارایی های سازمان باید با تامین کنندگان توافق شده و مستند شود.
الف ۱۵-۱-۲	پرداختن به امنیت درون توافقنامه های تامین کنندگان	کنترل: تمامی الزامات امنیت اطلاعات، باید با هر تامین کننده که امکان دسترسی، پردازش، ذخیره، مبادله یا تهیه اجزا زیرساخت فناوری اطلاعات برای اطلاعات سازمان را دارد، ایجاد و توافق شود.
الف ۱۵-۱-۳	زنجیره تامین فناوری اطلاعات و ارتباطات	کنترل: توافق نامه ها با تامین کنندگان باید شامل الزاماتی برای پرداختن به مخاطرات امنیت اطلاعات مربوط به زنجیره تامین خدمات و محصولات فناوری اطلاعات باشد.
الف ۱۵-۲ مدیریت تحول خدمت تامین کننده		
هدف: نگه داری یک سطح مورد توافق امنیت اطلاعات و تحویل خدمت در راستای توافق نامه های تامین کننده		

الف ۱۵-۲-۱	پایش و بازنگری خدمات تامین کننده	کنترل: سازمان ها باید تحویل خدمت تامین کننده را به صورت قاعده مند پایش و بازنگری و بازرسی کنند.
الف ۱۵-۲-۲	مدیریت تغییرات در خدمات تامین کننده	کنترل: تغییرات در ارائه خدمات توسط تامین کننده؛ شامل نگه داری و بهبود خط مشی ها امنیت اطلاعات، روش های اجرایی و کنترل موجود، باید با توجه به میزان بحرانی بودن اطلاعات کسب و کار، سیستم های و فرآیندهای مرتبط و برآورد مجدد مخاطرات، مدیریت شوند.
الف ۱۶ مدیریت رخداد امنیت اطلاعات		
الف ۱۶-۱ مدیریت رخدادهای امنیت اطلاعات و بهبودها		
هدف: حصول اطمینان از رویکردی استوار و موثر برای مدیریت رخدادهای امنیت اطلاعات، شامل ارتباط در مورد رویدادهای امنیتی و ضعف ها.		
الف ۱۶-۱-۱	مسئولیت ها و روش های اجرایی	کنترل: به منظور حصول اطمینان از یک پاسخ سریع، موثر و منظم به رخدادهای امنیت اطلاعات، مسئولیت های مدیریتی و روش های اجرایی باید ایجاد شوند.
الف ۱۶-۱-۲	گزارش دهی رویدادهای امنیت اطلاعات	کنترل: رویدادهای امنیت اطلاعات باید در کوتاه ترین زمان ممکن، از طریق مجرای مدیریتی مناسب، گزارش شوند.
الف ۱۶-۱-۳	گزارش دهی ضعف های امنیتی	کنترل: کارکنان و پیمانکارانی که از سیستم ها و خدمات اطلاعاتی سازمان استفاده می کنند، باید نسبت به توجه و گزارش دهی هر ضعف امنیتی مشاهده شده یا مورد سوظنن در سیستم ها یا خدمات، ملزم شوند.
الف ۱۶-۱-۴	ارزیابی و تصمیم برای رویدادهای امنیت اطلاعات	کنترل: رویدادهای امنیت اطلاعات باید ارزیابی شوند و باید تصمیم گیری شود که در صورت نیاز، به عنوان رخدادهای امنیت اطلاعات طبقه بندی شوند.
الف ۱۶-۱-۵	پاسخ به رخدادهای امنیت	کنترل: به رخدادهای امنیت اطلاعات باید مطابق با روش های اجرایی مستند، پاسخ داده شود.
الف ۱۶-۱-۶	یادگیری از رخدادهای امنیت اطلاعات	کنترل: دانش به دست آمده از تحلیل و برطرف کردن رخدادهای امنیت اطلاعات باید برای کاهش احتمال یا تاثیر رخدادهای آینده، استفاده شود.
الف ۱۶-۱-۷	گردآوری شواهد	کنترل: سازمان باید روش های اجرایی برای شناسایی، جمع آوری، اکتساب و حفاظت از اطلاعات، که می تواند به عنوان شواهد استفاده شود را، تعریف و به کار برد.
الف ۱۷ جنبه های امنیت اطلاعات مدیریت تداوم کسب و کار		
الف ۱۷-۱ تداوم امنیت اطلاعات		
هدف: تداوم امنیت اطلاعات باید در سیستم های مدیریت تداوم کسب و کار سازمان گنجانده شود.		

الف ۱۷-۱-۱	طرح ریزی تداوم امنیت اطلاعات	کنترل: سازمان باید نیازهای خود را برای امنیت اطلاعات و تداوم مدیریت اطلاعات در موقعیت های ناسازگار، به طور مثال در طول یک بحران یا فاجعه ، تعیین کند.
الف ۱۷-۱-۲	پیاده سازی تداوم امنیت اطلاعات	کنترل: برای حصول اطمینان از سطح مورد نیاز تداوم امنیت اطلاعات در حین یک موقعیت ناسازگار، سازمان باید فرآیندها، روش های اجرایی و کنترل هایی ایجاد، مستندسازی و پیاده سازی و نگه داری نماید.
الف ۱۷-۱-۳	بررسی، بازنگری و ارزشیابی تداوم امنیت اطلاعات	کنترل: سازمان باید کنترل های تداوم امنیت اطلاعات ایجاد و پیاده سازی شده را به منظور حصول اطمینان از معتبر و موثر بودنشان در حین موقعیت های ناسازگار، در بازه های زمانی منظم بررسی کند.
الف-۱۷-۲ افزونگی ها		
هدف: حصول اطمینان از دسترس پذیری امکانات پردازش اطلاعات.		
الف ۱۷-۲-۱	دسترس پذیری امکانات پردازش اطلاعات	کنترل: امکانات پردازش اطلاعات، باید برای برآورده ساختن الزامات دسترس پذیری یا افزونگی کافی پیاده سازی شوند.
الف ۱۸ انطباق		
الف ۱۸-۱ انطباق با الزامات قانونی و قراردادی		
هدف: پرهیز از نقض هر نوع قانون، مقررات، تعهدات آئین نامه ای یا قراردادی مرتبط با امنیت اطلاعات و هر الزام امنیتی		
الف ۱۸-۱-۱	شناسایی الزامات قانونی و قراردادی قابل اجرا	کنترل: تمامی مقررات قانون گزاری، الزامات آئین نامه ای، قراردادی مرتبط و رویکرد سازمان نسبت به برآورده سازی این الزامات، باید برای هر سامانه اطلاعاتی و سازمان، به وضوح شناسایی شده، تدوین شده و به روز نگه داشته شوند.
الف ۱۸-۱-۲	حقوق دارایی فکری	کنترل: به منظور حصول اطمینان از انطباق با الزامات قانون گزار، الزامات آئین نامه ای و قراردادی در مورد حقوق مالکیت معنوی و استفاده از محصولات نرم افزاری، روش های اجرایی مناسب باید پیاده سازی شوند.
الف ۱۸-۱-۳	حفاظت از سوابق	کنترل: سوابق باید با توجه به الزامات قانونی، آتین نامه ای، قراردادی و کسب و کار، در برابر گم شدن، تخریب، تحریف، دسترسی غیرمجاز و پخش غیرمجاز محافظت شوند.
الف ۱۸-۱-۴	حریم خصوصی و حفاظت از اطلاعات قابل شناسایی شخصی	کنترل: حریم خصوصی و حفاظت از اطلاعات قابل شناسایی شخصی باید آن گونه که در قوانین و آئین نامه های مرتبط الزام شده و هم چنین کاربرد پذیر است، تضمین شود.
الف ۱۸-۱-۵	قواعد کنترل های رمزنگاری	کنترل های رمزنگاری باید در انطباق با تمامی توافق نامه ها، قوانین و آئین نامه های مرتبط به کار گرفته شوند.

الف ۱۸-۲ بازنگری های امنیت اطلاعات		
هدف: حصول اطمینان از اینکه امنیت اطلاعات مطابق با خط مشی ها و روش های اجرایی سازمانی پیاده سازی و اجرا شده است.		
الف ۱۸-۲-۱	بازنگری مستقل امنیت اطلاعات	کنترل: رویکرد سازمان به مدیریت امنیت اطلاعات و پیاده سازی آن(به عنوان مثال اهداف کنترلی، کنترل ها، خط مشی ها، فرآیندها و روش های اجرایی امنیت اطلاعات) باید در فواصل زمانی طرح ریزی شده یا هنگامی که تغییرات عمده ای رخ دهد؛ به صورت مستقل بازنگری شود.
الف ۱۸-۲-۲	انطباق با خط مشی ها و استانداردهای امنیتی	کنترل: مدیران باید به طور منظم انطباق پردازش اطلاعات و روش های اجرایی در حیطه مسئولیتشان را با خط مشی های امنیتی مناسب، استانداردها و الزامات امنیتی دیگر، بازنگری کنند.
الف ۱۸-۲-۳	بررسی انطباق فنی	کنترل: به منظور انطباق بت خط مشی ها و استانداردهای امنیت اطلاعات سازمان، باید سامانه های اطلاعاتی به صورت منظم بازنگری شود.