استاندارد ایزو ۲۷۰۰۱:۲۰۱۳

ISO/IEC 27001:2013

محمد مهدی واعظی نژاد

Mvaezi.ir

Tel: 09360895848

eMail: Mahdivaezi61@yahoo.com

نسخه الکترونیک

به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید، از روح خود در او دمید و او را خلیفه خویش در زمین قرار داد و پیامبرانش را با دلایل آشکار فرو فرستاد تا انسان‌ها را به سعادت و هدایت، بر پایه تفکر و تعقل، رهنمون گردانند.

فهرست مطالب

مقدمه ۵
پیشگفتار ۶
۰. مقدمه ۷
۱,۰کلیات ۷
۲,۰سازگاری با سایر استانداردهای سیستم مدیریت ۸
۱. قلمرو ۹
۲. مراجع اصلی ۹
۳. اصطلاحات و تعاریف ۹
۴. چارچوب سازمان ۹
۱,۴شناخت سازمان و چارچوب آن ۹
۲,۴ شناخت نیازها و انتظارات طرف‌های ذینفع ۱۰
۳,۴تعیین قلمرو سیستم مدیریت امنیت اطلاعات..... ۱۰
۴,۴ سیستم مدیریت امنیت اطلاعات ۱۰
۵. رهبری ۱۰
۱,۵رهبری و تعهد..... ۱۰
۲,۵خط‌مشی ۱۱
۳,۵نقش‌های سازمانی، مسئولیت‌ها و اختیارات ۱۲
۶. طرح‌ریزی ۱۲
۱,۶اقداماتی برای درنظر گرفتن مخاطرات و فرصت‌ها ۱۲
۱,۱,۶ کلیات ۱۲
۲,۱,۶ارزیابی مخاطرات امنیت اطلاعات..... ۱۳
۳,۱,۶برطرف‌سازی مخاطرات امنیت اطلاعات..... ۱۳
۲,۶ اهداف امنیت اطلاعات و طرح‌ریزی برای دستیابی به آنها..... ۱۴
۷. پشتیبانی ۱۵
۱,۷منابع ۱۵
۲,۷صلاحیت ۱۵
۳,۷ آگاه‌سازی ۱۶
۴,۷ ارتباطات ۱۶

۵,۷اطلاعات مستند ۱۶
۱,۵,۷کلیات ۱۶
۲,۵,۷ایجاد و به روزرسانی ۱۷
۳,۵,۷کنترل اطلاعات مستند ۱۷
۸. عملیات ۱۸
۱,۸طرح‌ریزی و کنترل عملیات ۱۸
۲,۸ ارزیابی مخاطرات امنیت اطلاعات ۱۸
۳,۸ برطرف‌سازی مخاطرات امنیت اطلاعات ۱۸
۹. ارزشیابی عملکرد ۱۹
۱,۹ پایش، اندازه‌گیری، تحلیل و ارزشیابی ۱۹
۲,۹ ممیزی داخی ۱۹
۳,۹ بازنگری مدیریت ۲۰
۱۰. بهبود ۲۱
۱,۱۰عدم انطباق و اقدام اصلاحی ۲۱
۲,۱۰بهبود مستمر ۲۲
کتابنامه ۳۳

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 27001که 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.

محمد مهدی واعظی نژاد

خرداد ۱۳۹۳

پیشگفتار

سازمان بین‌المللی استاندارد (ISO) و کمیسیون بین‌المللیالکتروتکنیک (IEC)، سیستمی تخصصی را جهت استانداردسازی در سطح دنیا ایجاد کرده‌اند. 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 وIEC، 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 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

۱,۰کلیات

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 فراهم‌آوریالزامات 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.

۲,۰سازگاری 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

۱,۴شناخت سازمان و چارچوب 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.

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.

۳,۴تعیین 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

۱,۵رهبری 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.

۲,۵خط‌مشی

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.

۳,۵نقش‌های 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

۱,۶اقداماتی 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.

۲,۱,۶ارزیابی 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.

۳,۱,۶برطرف‌سازی 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

۱,۷منابع

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

۲,۷صلاحیت

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.

۵,۷اطلاعات مستند

۱,۵,۷کلیات

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.

۲,۵,۷ایجاد 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.

۳,۵,۷کنترل 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،۸طرح‌ریزی 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، اقدام‌هاییرا 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 داخی

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،۱۰عدم 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.

۲,۱۰بهبود 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.۹.۲،۱	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.۹.۲،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 حقوق دسترسی کاربر	کنترل: مالکان دارایی‌ها باید حقوق دسترسی کاربران را در فواصل زمانی منظم بازنگری کنند.
الف.۹.۲،۶	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	کار در نواحی امن	کنترل: رویه‌هایی برای کار در نواحی امن، باید طراحی شده و به کار گرفته شود.
الف.۶,۱,۱۱	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 ابنیه	کنترل: برای دارایی‌های خارج از ابنیه، باید با توجه به مخاطرات مختلف ناشی از انجام کار در خارج از بناهای 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: واقعه‌نگاری و پایش		
هدف: ثبت رویدادها و ایجاد شواهد		
الف.۱,۴,۱۲	واقعه‌نگاری رویداد	کنترل: واقعه‌نگاری 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 واقعه‌نگاری 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 واقعه‌نگاری 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	کنترل: دستکاری در بسته‌های نرم افزاری باید مسدود شده و محدود به تغییرات

	در بسته‌های نرم افزاری	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.
الف.۹,۲,۱۴	آزمون پذیرش سیستم	کنترل: برنامه‌های آزمون پذیرش و معیارهای مربوطه باید برای سیستم‌های اطلاعاتی جدید، به روز رسانی‌ها و نسخه‌های جدید ایجاد شود.
الف.۳,۱۴: 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 وکنترل‌های 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: افزونگی‌ها		
هدف: حصول اطمینان از دسترس‌پذیری امکانات پردازش اطلاعات		
الف.۱,۲,۱۷	دسترس‌پذیری امکانات پردازش اطلاعات	کنترل: امکانات پردازش اطلاعات باید با افزونگی‌های 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	کنترل: تمامی الزامات قانونی، حقوقی، مقرراتی، قراردادی مرتبط و رویکرد سازمان

	قراردادی قابل اجرا	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 –آیین‌کارکنترل‌های 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- دستورالعمل‌هایISO/IEC، بخش ۱، مکمل‌های تلفیقی ISO– رویه‌های مختصISO، ۲۰۱۲

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Reference number
ISO/IEC 27001:2013(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**

0 Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Context of the organization **1**
4.1 Understanding the organization and its context 1
4.2 Understanding the needs and expectations of interested parties 1
4.3 Determining the scope of the information security management system 1
4.4 Information security management system 2

5 Leadership **2**
5.1 Leadership and commitment 2
5.2 Policy 2
5.3 Organizational roles, responsibilities and authorities 3

6 Planning **3**
6.1 Actions to address risks and opportunities 3
6.2 Information security objectives and planning to achieve them 5

7 Support **5**
7.1 Resources 5
7.2 Competence 5
7.3 Awareness 5
7.4 Communication 6
7.5 Documented information 6

8 Operation **7**
8.1 Operational planning and control 7
8.2 Information security risk assessment 7
8.3 Information security risk treatment 7

9 Performance evaluation **7**
9.1 Monitoring, measurement, analysis and evaluation 7
9.2 Internal audit 8
9.3 Management review 8

10 Improvement **9**
10.1 Nonconformity and corrective action 9
10.2 Continual improvement 9

Annex A (normative) **Reference control objectives and controls** **10**

Bibliography **23**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27001:2005), which has been technically revised.

0 Introduction

0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Information technology — Security techniques — Information security management systems — Requirements

1 Scope

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2; and

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; and

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization; and

g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this International Standard; and

b) reporting on the performance of the information security management system to top management.

NOTE Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

1) integrate and implement the actions into its information security management system processes; and

2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

1) the risk acceptance criteria; and

2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

2) identify the risk owners;

d) analyses the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

e) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.

NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000[5].

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be communicated; and

e) be updated as appropriate.

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

f) what will be done;

g) what resources will be required;

h) who will be responsible;

i) when it will be completed; and

j) how the results will be evaluated.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions may include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the information security management system requirements.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who shall communicate; and

e) the processes by which communication shall be effected.

7.5 Documented information

7.5.1 General

The organization's information security management system shall include:

a) documented information required by this International Standard; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:

1) the size of organization and its type of activities, processes, products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE The methods selected should produce comparable and reproducible results to be considered valid.

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated; and

f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization's own requirements for its information security management system; and

2) the requirements of this International Standard;

b) is effectively implemented and maintained.

The organization shall:

c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

d) define the audit criteria and scope for each audit;

e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

f) ensure that the results of the audits are reported to relevant management; and

g) retain documented information as evidence of the audit programme(s) and the audit results.

9.3 Management review

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results; and

4) fulfilment of information security objectives;

d) feedback from interested parties;

e) results of risk assessment and status of risk treatment plan; and

f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.

10 Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it; and

2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity; and

3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

f) the nature of the nonconformities and any subsequent actions taken, and

g) the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

Annex A
(normative)

Reference control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.

Table A.1 — Control objectives and controls

A.5 Information security policies		
A.5.1 Management direction for information security		
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	*Control* The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6 Organization of information security		
A.6.1 Internal organization		
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.6.1.3	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.4	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.5	Information security in project management	*Control* Information security shall be addressed in project management, regardless of the type of the project.
A.6.2 Mobile devices and teleworking		
Objective: To ensure the security of teleworking and use of mobile devices.		

Table A.1 *(continued)*

A.6.2.1	Mobile device policy	*Control* A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
A.6.2.2	Teleworking	*Control* A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.
A.7 Human resource security		
A.7.1 Prior to employment		
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.		
A.7.1.1	Screening	*Control* Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
A.7.1.2	Terms and conditions of employment	*Control* The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.
A.7.2 During employment		
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1	Management responsibilities	*Control* Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
A.7.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
A.7.2.3	Disciplinary process	*Control* There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
A.7.3 Termination and change of employment		
Objective: To protect the organization's interests as part of the process of changing or terminating employment.		
A.7.3.1	Termination or change of employment responsibilities	*Control* Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
A.8 Asset management		
A.8.1 Responsibility for assets		

Table A.1 *(continued)*

Objective: To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1	Inventory of assets	*Control* Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
A.8.1.2	Ownership of assets	*Control* Assets maintained in the inventory shall be owned.
A.8.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.
A.8.1.4	Return of assets	*Control* All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
A.8.2 Information classification		
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1	Classification of information	*Control* Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
A.8.2.2	Labelling of information	*Control* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.2.3	Handling of assets	*Control* Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.3 Media handling		
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
A.8.3.1	Management of removable media	*Control* Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
A.8.3.2	Disposal of media	*Control* Media shall be disposed of securely when no longer required, using formal procedures.
A.8.3.3	Physical media transfer	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.
A.9 Access control		
A.9.1 Business requirements of access control		

Table A.1 *(continued)*

Objective: To limit access to information and information processing facilities.		
A.9.1.1	Access control policy	*Control* An access control policy shall be established, documented and reviewed based on business and information security requirements.
A.9.1.2	Access to networks and network services	*Control* Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
A.9.2 User access management		
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	User registration and de-registration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.3	Management of privileged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users' access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
A.9.3 User responsibilities		
Objective: To make users accountable for safeguarding their authentication information.		
A.9.3.1	Use of secret authentication information	*Control* Users shall be required to follow the organization's practices in the use of secret authentication information.
A.9.4 System and application access control		
Objective: To prevent unauthorized access to systems and applications.		
A.9.4.1	Information access restriction	*Control* Access to information and application system functions shall be restricted in accordance with the access control policy.
A.9.4.2	Secure log-on procedures	*Control* Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

Table A.1 *(continued)*

A.9.4.3	Password management system	*Control* Password management systems shall be interactive and shall ensure quality passwords.
A.9.4.4	Use of privileged utility programs	*Control* The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.9.4.5	Access control to program source code	*Control* Access to program source code shall be restricted.
A.10 Cryptography		
A.10.1 Cryptographic controls		
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.		
A.10.1.1	Policy on the use of cryptographic controls	*Control* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.10.1.2	Key management	*Control* A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
A.11 Physical and environmental security		
A.11.1 Secure areas		
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.		
A.11.1.1	Physical security perimeter	*Control* Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
A.11.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms and facilities shall be designed and applied.
A.11.1.4	Protecting against external and environmental threats	*Control* Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
A.11.1.5	Working in secure areas	*Control* Procedures for working in secure areas shall be designed and applied.
A.11.1.6	Delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Table A.1 *(continued)*

A.11.2 Equipment		
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
A.11.2.1	Equipment siting and protection	*Control* Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.11.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
A.11.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.11.2.5	Removal of assets	*Control* Equipment, information or software shall not be taken off-site without prior authorization.
A.11.2.6	Security of equipment and assets off-premises	*Control* Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
A.11.2.7	Secure disposal or re-use of equipment	*Control* All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
A.11.2.8	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.
A.11.2.9	Clear desk and clear screen policy	*Control* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
A.12 Operations security		
A.12.1 Operational procedures and responsibilities		
Objective: To ensure correct and secure operations of information processing facilities.		
A.12.1.1	Documented operating procedures	*Control* Operating procedures shall be documented and made available to all users who need them.
A.12.1.2	Change management	*Control* Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

Table A.1 *(continued)*

A.12.1.3	Capacity management	*Control* The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
A.12.1.4	Separation of development, testing and operational environments	*Control* Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.
A.12.2 Protection from malware		
Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1	Controls against malware	*Control* Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
A.12.3 Backup		
Objective: To protect against loss of data.		
A.12.3.1	Information backup	*Control* Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
A.12.4 Logging and monitoring		
Objective: To record events and generate evidence.		
A.12.4.1	Event logging	*Control* Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
A.12.4.2	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.
A.12.4.3	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
A.12.4.4	Clock synchronisation	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.
A.12.5 Control of operational software		
Objective: To ensure the integrity of operational systems.		
A.12.5.1	Installation of software on operational systems	*Control* Procedures shall be implemented to control the installation of software on operational systems.
A.12.6 Technical vulnerability management		
Objective: To prevent exploitation of technical vulnerabilities.		

Table A.1 *(continued)*

A.12.6.1	Management of technical vulnerabilities	*Control* Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
A.12.6.2	Restrictions on software installation	*Control* Rules governing the installation of software by users shall be established and implemented.
A.12.7 Information systems audit considerations		
Objective: To minimise the impact of audit activities on operational systems.		
A.12.7.1	Information systems audit controls	*Control* Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.
A.13 Communications security		
A.13.1 Network security management		
Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1	Network controls	*Control* Networks shall be managed and controlled to protect information in systems and applications.
A.13.1.2	Security of network services	*Control* Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
A.13.1.3	Segregation in networks	*Control* Groups of information services, users and information systems shall be segregated on networks.
A.13.2 Information transfer		
Objective: To maintain the security of information transferred within an organization and with any external entity.		
A.13.2.1	Information transfer policies and procedures	*Control* Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
A.13.2.2	Agreements on information transfer	*Control* Agreements shall address the secure transfer of business information between the organization and external parties.
A.13.2.3	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.

Table A.1 *(continued)*

A.13.2.4	Confidentiality or non-disclosure agreements	*Control* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
A.14 System acquisition, development and maintenance		
A.14.1 Security requirements of information systems		
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.		
A.14.1.1	Information security requirements analysis and specification	*Control* The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
A.14.1.2	Securing application services on public networks	*Control* Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
A.14.1.3	Protecting application services transactions	*Control* Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.14.2 Security in development and support processes		
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.		
A.14.2.1	Secure development policy	*Control* Rules for the development of software and systems shall be established and applied to developments within the organization.
A.14.2.2	System change control procedures	*Control* Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
A.14.2.3	Technical review of applications after operating platform changes	*Control* When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.14.2.4	Restrictions on changes to software packages	*Control* Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
A.14.2.5	Secure system engineering principles	*Control* Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

Table A.1 *(continued)*

A.14.2.6	Secure development environment	*Control* Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
A.14.2.7	Outsourced development	*Control* The organization shall supervise and monitor the activity of outsourced system development.
A.14.2.8	System security testing	*Control* Testing of security functionality shall be carried out during development.
A.14.2.9	System acceptance testing	*Control* Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.
A.14.3 Test data		
Objective: To ensure the protection of data used for testing.		
A.14.3.1	Protection of test data	*Control* Test data shall be selected carefully, protected and controlled.
A.15 Supplier relationships		
A.15.1 Information security in supplier relationships		
Objective: To ensure protection of the organization's assets that is accessible by suppliers.		
A.15.1.1	Information security policy for supplier relationships	*Control* Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
A.15.1.2	Addressing security within supplier agreements	*Control* All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
A.15.1.3	Information and communication technology supply chain	*Control* Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
A.15.2 Supplier service delivery management		
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.		
A.15.2.1	Monitoring and review of supplier services	*Control* Organizations shall regularly monitor, review and audit supplier service delivery.
A.15.2.2	Managing changes to supplier services	*Control* Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Table A.1 *(continued)*

A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.3	Reporting information security weaknesses	*Control* Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
A.16.1.4	Assessment of and decision on information security events	*Control* Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	*Control* Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6	Learning from information security incidents	*Control* Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7	Collection of evidence	*Control* The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
A.17 Information security aspects of business continuity management		
A.17.1 Information security continuity		
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.		
A.17.1.1	Planning information security continuity	*Control* The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2	Implementing information security continuity	*Control* The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Table A.1 *(continued)*

A.17.1.3	Verify, review and evaluate information security continuity	*Control* The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
A.17.2 Redundancies		
Objective: To ensure availability of information processing facilities.		
A.17.2.1	Availability of information processing facilities	*Control* Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
A.18 Compliance		
A.18.1 Compliance with legal and contractual requirements		
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.		
A.18.1.1	Identification of applicable legislation and contractual requirements	*Control* All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
A.18.1.2	Intellectual property rights	*Control* Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
A.18.1.3	Protection of records	*Control* Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.
A.18.1.4	Privacy and protection of personally identifiable information	*Control* Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
A.18.1.5	Regulation of cryptographic controls	*Control* Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
A.18.2 Information security reviews		
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.		
A.18.2.1	Independent review of information security	*Control* The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

Table A.1 *(continued)*

A.18.2.2	Compliance with security policies and standards	*Control* Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
A.18.2.3	Technical compliance review	*Control* Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Bibliography

[1] ISO/IEC 27002:2013, *Information technology — Security Techniques — Code of practice for information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

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

[4] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[5] ISO 31000:2009, *Risk management — Principles and guidelines*

[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement – Procedures specific to ISO*, 2012

ICS 35.040
Price based on 23 pages