مرکز مشاوره و اطلاع رسانی

سیستم کاران

ISO 28000:2007

ویژگی سیستم های

مدیریت امنیت زنجیره تامین

تهیه کننده :

مرکز مشاوره و اطلاع رسانی سیستم کاران

WWW.SYSTEMKARAN.ORG

فهرست

پیش گفتار

ISO (سازمان جهانی استاندارد) مرجع جهانی متشکل از موسسات ملی استاندارد کشورهای مختلف (سازمان های عضو ISO) می باشد. کار تهیه استانداردهای جهانی به طور رایج از طریق کمیته های فنی آن صورت می پذیرد. هر یک از سازمان های عضو بنا بر علاقه در موضوعی که برای آن یک کمیته تشکیل شده حق مشارکت در آن کمیته را دارد. سازمان های بین المللی، دولتی یا غیر دولتی نیز ضمن هماهنگی با سازمان جهانی استاندارد در این فعالیت مشارکت می نمایند.

سازمان جهانی استاندارد در مورد استانداردهای الکتروتکنیکی با کمیسیون جهانی الکتروتکنیک (IEC) در ضمینه استاندارد سازی الکتروتکنیکی کلیه موضوعات همکاری نزدیک دارد.

پیش نویس استانداردهای جهانی بر طبق مقررات وضع شده در قسمت بخشنامه ISO/IEC تدوین می گردد.

وظیفه اصلی کمیته های فنی تهیه استانداردهای بین المللی می باشد. پیش نویس استانداردهای جهانی مورد تایید کمیته های فنی دربین کشورهای عضو به منظور رای گیری توزیع می شود.

انتشار یک مدرک به عنوان استاندارد جهانی نیاز به تایید حداقل ۷۵٪ از کشورهای عضو که در رای گیری شرکت می نمایند خواهد داشت.

باید توجه داشت که ممکن است بعضی از قسمت های این مدرک تحت حق امتیاز به ثبت رسیده باشد. سازمان جهانی استاندارد مسئولیت شناسایی این گونه قسمت ها را به صورت کلی یا جزئی نمی پذیرد.

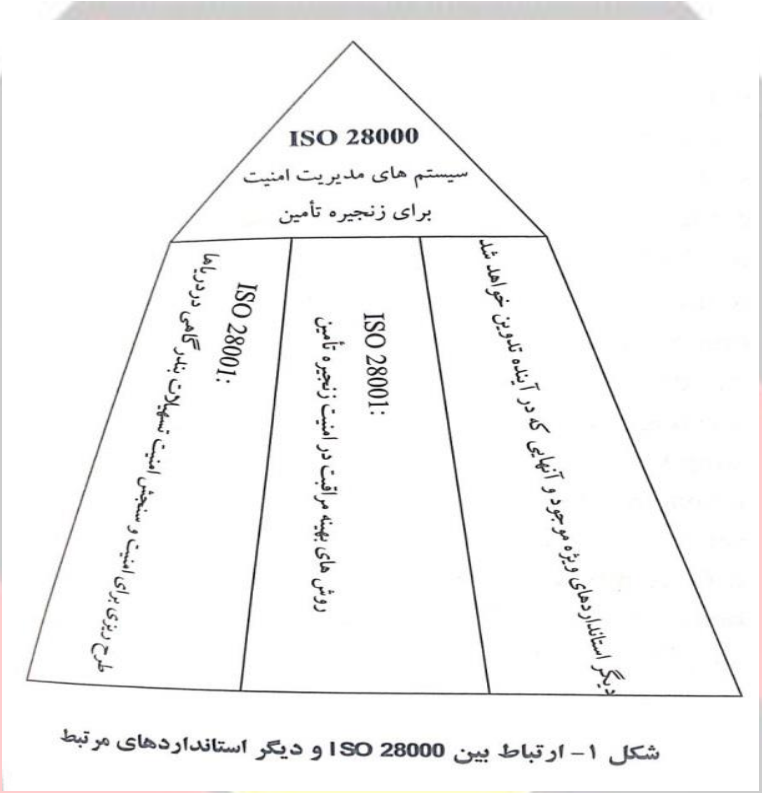
ایزو ۲۸۰۰۰ توسط کمیته فنی ISO/TC8 (کشتی ها و تکنولوژی دریایی) با همکاری دیگر کمیته های فنی مسئول و درگیر با معضلات خاص زنجیره تامین، تهیه شده است. این ویرایش اول از استاندارد ISO28000 مدرک ISO/PAS28000:2005 را لغو نموده و جایگزین آن می گردد و از نظر نکات فنی مورد تجدید نظر قرار گرفته است.

مقدمه

این استاندارد بین المللی در پاسخگویی به درخواست صنعت برای یک استاندارد مدیریت امنیت تدوین شده است. هدف نهایی از آن بهبود امنیت زنجیره تامین می باشد. این (استاندارد) یک استاندارد سطح بالای مدیریت می باشد که یم سازمان را قادر به استقرار یک سیستم مدیریت امنیت برای کل زنجیره تامین می نماید. این استاندارد نیاز به انجام توسط سازمان از فضای امنیتی که تحت آن عمل می کند دارد تا تعیین نماید چنانچه تمهیدات امنیتی کافی در سازمان به اجرا گذاشته شده و دریابد که چه نیازهای ثانوی دیگری در حال حاضر وجود دارد که سازمان ملزم به رعایت آنها می باشد.

اگر نیازهای امنیتی طی این فرایند شناسایی شوند سازمان موظف است مکانیزم ها و فرآیندهایی را که این نیازها را برآورده می سازد مستقر نماید. از آنجایی که زنجیره های تامین ماهیتی سیال متغییر یا زمان دارند

برخی سازمانها که زنجیره های چندگانه تامین را مدیریت می کنند ممکن است انتظار داشته باشند تا ارائه کنندگان خدمات به آنها استاندارد ISO امنیت زنجیره تامین و یا استانداردهای مرتبط دولتی را به عنوان شرطی برای قرار گرفتن در زنجیره تامین به منظور ساده کردن مدیریت امنیت طبق آنچه در شکل ۱ نشان داده شده لحاظ نماید.



شکل ۱- ارتباط بین ISO 28000 و دیگر استانداردهای مرتبط

هدف از این استاندارد بین المللی کاربرد آن در مواردی است که زنجیره تامین یک سازمان به مدیریت به صورت ایمن دارای امنیت نیاز داشته باشد. یک نگرش رسمی به مدیریت امنیت می تواند مستقیما به توانایی تجاری و اعتبار سازمان کمک نماید.

رعایت یک استاندارد جهانی به خودی خود باعث مبرا شدن از الزامات قانونی نمی گردد. برای سازمان ها در صورت تمایل رعایت سیستم مدیریت امنیت با این استاندارد بین المللی ممکن است از طریق فرآیند ممیزی خارجی یا داخلی مورد صحه گذاری گیرد.

این استاندارد جهانی بر مبنای چهارچوب ISO مورد استفاده در استاندارد ISO14001:2004 به دلیل رویکرد مبتنی بر ریسک سیستم های مدیریت تدوین شده است. اگر چه سازمانهایی که از رویکرد فرآیندی برای سیستم های مدیریت (به عنوان مثال ISO9001:2000) بهره گرفته باشند، ممکن است سیستم مدیریت موجود خود را به عنوان پایه مبنا برای سیستم مدیریت امنیت طبق آنچه که در این استاندارد جهانی پیشنهاد شده مورد قرار دهند. این استاندارد بین المللی قصد ندارد نیازهای دولتی و استانداردهای مدیریت امنیت

زنجیره تامین را که سازمان در حال حاضر برای رعایت آنها گواهی دریافت کرده مجدد تکرار نماید. (سازمان مجبور به دوباره کاری گردد).

یادآوری: این استاندارد بین المللی بر مبنای روش طرح ریزی (Plan)، اجرا (Do)، بررسی (Check) و اقدام (Act) تدوین شد که اصطلاحا PDCA خوانده می شود. PDCA را می توان به اختصار به شرح زیر تشریح نمود.

بررسی (به منظور کنترل) (Check) : پایش فرآیندها بر مبنای خط مشی امنیتی، اهداف کلان (انتظارات)، اهداف خرد، اقدامات قانونی و دیگر الزامات و گزارش نتایج.

اقدام (با هدف بازنگری) (؛) : انجام اقدامات برای بهبود مستمرعملکرد سیستم مدیریت امنیت (در صورت نیاز اقدام اصلاحی انجام شود).

طرح ریزی (Plan) : تعیین اهداف و فرآیندهای مورد نیاز برای دستیابی به نتایج، طبق خط مشی امنیت سازمان

اجرا (Do) : استقرار فرآیندهای مورد نظر

ویژگی سیستم های مدیریت امنیت برای زنجیره تامین

۱- دامنه کاربرد

این استاندارد بین المللی نیازهای یک سیستم مدیریت امنیت شامل آن جنبه هایی را که برای تضمین امنیت زنجیره تأمین بحرانی می باشد. مشخص می نماید.

مدیریت امنیت با بسیاری دیگر از جنبه های مدیریت تجاری مرتبط می باشد. جنبه ها شامل کلیه فعالیتهایی می باشد که توسط سازمان کنترل شده و یا از آن متاثر میشود و بر روی زنجیره تأمین تأثیر گذار می باشد.

جنبه های دیگر می بایست به طور مستقیم هر جا و هر زمان که بر مدیریت امنیت تأثیر گذار باشد مورد کنترل (بررسی) قرار گیرند. از جمله این موارد جابجایی کالا در طول زنجیره تأمین می باشد.

این استاندارد بین المللی برای همه سازمانها اعم از کوچک، چند ملیتی در بخش تولید، خدمات انبارش و جابجایی در هر مقطع از تولید و زنجیره تأمین که قصد داشته باشد یکی از اهداف زیر را محقق سازد کاربرد دارد:

الف) یک سیستم مدیریت امنیت را دایر کرده به کار گیرد، نگهداری و بهینه سازد.

ب) از انطباق با خط مشی مدیریت امنیت به گونه ای که اعلام شده اطمینان حاصل نماید.

ج) این انطباق را به دیگران نشان دهد.

د) در صدد مورد تأیید قرار گرفتن / ثبت سیستم مدیریت امنیت توسط یک مرجع مورد تأیید صدور گواهی شخص ثالث باشد و یا؛

ه) انطباق با این استاندارد بین المللی را شخصاً تعیین کرده و خود اظهاری نماید.

برای برخی نیازهای این استاندارد بین المللی کدهای مربوط به قوانین و ضوابط کنترل وجود دارد.

هدف این استاندارد بین المللی نشان دادن (اثبات نمودن) مجدد وجود انطباق در سازمان نمی باشد.

سازمان هایی که دریافت گواهی شخص ثالث را به عنوان گزینه انتخاب می کنند همچنین نشان می دهند که آنها به طورقابل توجه (بارز) به امنیت زنجیره تامین کمک می نمایند.

۲- مراجع الزامی

هیچ مرجع الزامی موردنظر نمی باشد این بند (از استاندارد) صرفا به دلیل رعایت ساختار شماره گذاری دیگر استانداردهای سیستم مدیریت گنجانده شده است.

۳- تعاریف و واژگان

برای کاربرد این استاندارد، تعاریف و واژگان زیر کاربرد دارد:

۳-۱- امکانات

کارخانه، ماشین آلات، ملک، ساختمان ها، وسایل نقلیه، کشتی ها، امکانات بندری و وسایر موارد زیر ساختاری یا کارخانه و سیستم های مرتبط که دارای وظایف و یا خدمات تجاری قابل اندازه گیری باشند. (خروجی فعالیت آنها قابل اندازه گیری باشد)

یادآوری: این تعریف شامل کدهای نرم افزاری که برای ارائه امنیت و کاربرد مدیریت امنیت ضروری (حیاتی) می باشد نیز می گردد.

۳-۲- امنیت

مقاومت با عمل (اعمال) عمدی یا بدون مجوز به منظور صدمه رسانی به، و یا توسط، زنجیره تامین.

۳-۳- مدیریت امنیت

فعالیت های سازماندهی شده و هماهنگ و فعالیت هایی که توسط آنها سازمان به طور منطقی ریسک ها و تهدیدهای بالقوه خود و تاثیرات ناشی از آنها را مدیریت می کند.

۳-٤- هدف کلان (انتظار کلی از) مدیریت امنیت

دستاورد یا خروجی مشخص مورد انتظار از امنیت به منظور رعایت خط مشی مدیریت امنیت.

یادآوری : لازم است چنین خروجی هایی به طور مستقیم یا غیر مستقیم به تحقق محصول یا ارائه خدمات توسط کل فعالیت تجاری (سازمان) به مشتریان یا کاربران نهایی آن مرتبط باشد.

۳-۵- خط مشی مدیریت امنیت

نیات کلی گرایشها و جهت گیری یک سازمان در ارتباط با امنیت و چهار چوب کنترلی فعالیتهای مرتبط با امنیت و فعالیت های ناشی از آن و همخوان با خط مشی (کلی) سازمان و الزامات قانونی

۳-۶- برنامه های مدیریت امنیت

راه هایی که توسط آن اهداف کلان مدیریت امنیت بر آورده می شود.

۳-۷- هدف (خرد) مدیریت امنیت

سطح مشخصی از عملکرد مورد نیاز برای رسیدن به اهداف کلان مدیریت امنیت

۳-۸- ذینفع

شخصی با موجودیتی که در عملکرد سازمان، موفقیت و تاثیر فعالیت آن دارای منافع باشد.

یادآوری: مثال های ذینفعان شامل مشتریان، سهامداران، سرمایه گذاران بیمه گذاران، قانون گذاران، مقامات دولتی، کارکنان، پیمانکاران تأمین کنندگان سازمان های کارگری و یا جامعه

۳-۹- زنجیره تامین

مجموعه منابع متصل به هم و فعالیت هایی که با شناسایی مواد اولیه آغاز و به تحویل محصولات و خدمات به مصرف کننده نهایی، توسط انواع وسایل جابجایی حمل و نقل می انجامد.

یادآوری: زنجیره تامین میتواند شامل فروشندگان، امکانات تولیدی ارائه کنندگان خدمات بازرگانی و جابجایی، مراکز توزیع داخلی، توزیع کنندگان، عمده فروشان و دیگر عواملی با شد که به مصرف کننده نهایی ختم می شود، باشد.

۳-۹-۱- پایین دستی

منظور اقدامات، فرآیندها و جابجایی محموله در زنجیره تأمین پس از آنکه محموله حیطه کنترلی مستقیم سازمان را ترک کند، شامل و نه محدود به بیمه منابع مالی مدیریت داده ها بسته بندی انبارش و انتقال محموله

۳-۹-۲- بالا دستی

منظور اقدامات، فرآیندها جابجایی محموله در زنجیره تأمین قبل از آن که محموله وارد حیطه کنترلی مستقیم سازمان شود، شامل و نه محدود به بیمه، منابع مالی مدیریت داده ها بسته بندی انبارش و انتقال محموله.

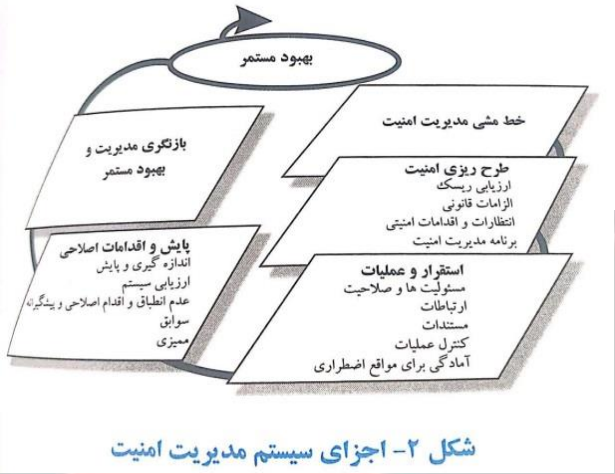
۳-۱۰- مدیریت ارشد شخص یا گروه اشخاص که سازمان را در بالاترین سطح هدایت و کنترل می کنند.

یادآوری: مدیریت ارشد به خصوص در سازمان های بزرگ ممکن است آن گونه که در این استاندارد تشریح می شود شخصاً در گیر (مسئول) نباشد اما پاسخگویی (مسئولیت) مدیریت ارشد در کنترل تمامی زنجیره تأمین باید نشان داده شود (قابل تعریف تشخیص باشد).

۳-۱۱- بهبود مستمر

فرآیند اجرا شده برای افزایش توان مستقیم مدیریت امنیت به منظور دستیابی به بهبود کلی عملکرد امنیتی (سازمان) در همخوانی با خط مشی امنیتی سازمان.

٤- اجزای سیستم مدیریت امنیت



شکل ۲- اجزای سیستم مدیریت امنیت

٤-۱- الزامات عمومی

سازمان باید یک سیستم مدیریت امنیت مؤثر را به وجود آورد، مستندسازی نماید، استقرار دهد و نگهداری و به طور مستمر بهبود بخشد تا تهدیدات امنیتی را شناسایی کرده، ریسکها را ارزیابی نموده و طبعات آنها را تحت کنترل درآورده و هر گونه زیان احتمالی را در راستای الزامات قید شده در کل بند ٤ افزایش دهد.

سازمان باید دامنه کاربرد سیستم مدیریت امنیت خود را تعریف نماید. چنانچه سازمان این گزینه را انتخاب کند که هر فرآیندی را که در انطباق با این الزامات است برون سپاری نماید، سازمان باید از تحت کنترل بودن این گونه فرآیندها اطمینان حاصل نماید.

کنترل های لازم و مسئولیت های مربوط به این گونه فرآیندهای برون سپاری شده باید در سیستم مدیریت امنیت شناسایی شود.

٤-۲- خط مشی مدیریت امنیت

مدیریت ارشد سازمان باید یک خط مشی کلی برای مدیریت امنیت را به اجرا گذارد. خط مشی باید:

الف) همخوان با دیگر خط مشی های سازمان باشد.

ب) چهارچوبی را ارائه نماید که انتظارات مشخص مدیریت امنیت اهداف و برنامه ها را در ارتباط با سیستم مدیریت امنیت تهیه نماید.

ج) همخوان با چهارچوب کلی مدیریت ریسک و تهدید امنیت سازمان باشد.

د) مناسب با (ماهیت) تهدیدات برای سازمان و مقیاس عملیات آن (سازمان) باشد.

ه) به طور شفاف انتظارات کلی گسترده سازمان را بیان نماید.

و) در برگیرنده تو رنده تعهد برای بهبود مستمر فرآیند مدیریت امنیت باشد.

ز) دربرگیرنده تعهد برای رعایت قوانین جاری مورد کاربرد، الزامات دولتی و کنترلی و دیگر الزاماتی

باشد که سازمان باید آنها را رعایت کند.

ح) توسط مدیریت ارشد به طور قابل رویت تایید شده باشد.

ط) مستند سازی شده، به اجرا گذشته شده و حفظ شود.

ی) به کلیه پرسنل مرتبط، شخص های ثالث، از جمله پیمانکاران و بازدید کنندگان انتقال داده شود با این قصد که افراد نسبت به تعهدات خود در ارتباط با مدیریت امنیت (سازمان) آگاهی یابند.

ک) در هر جا که مناسب باشد در اختیار ذینفعان قرار گیرد.

ل) امکان بازنگری سیستم مدیریت امنیت برای هنگامی که سازمان (توسط فرد یا سازمانی) خریداری شود، با دیگر سازمانها ادغام شود و یا هر تغییری در دامنه کاربرد فعالیت تجاری سازمان پیش آید که امکان تاثیر گذاری بر ادامه آن (سیستم مدیریت امنیت) داشته باشد را فراهم سازد.

یادآوری: سازمان ممکن است این گزینه را انتخاب نماید که یک خط مشی مشروح برای مدیریت امنیت خود برای کاربرد داخلی تهیه نماید که طی آن اطلاعات کافی و جهت گیری برای هدایت سیستم مدیریت امنیت که ممکن است بعضی قسمت های آن محرمانه باشد و یک خلاصه (غیر محرمانه تهیه نماید که در برگیرنده اهداف کلان سیستم مدیریت امنیت باشد و آن را برای توزیع به ذینفعان و دیگر سازمان های علاقه مند در نظر گیرد.

٤-۳- ارزیابی ریسک امنیت و طرح ریزی

٤-۳-۱- ارزیابی ریسک امنیت

سازمان باید روش های اجرایی برای شناسایی و ارزیابی جاری تهدیدات امنیت و ریسک ها و تهدیدات مرتبط با مدیریت امنیت و شناسایی و به اجراءِ گذاشتن اقدامات مدیریتی کنترل، تهیه و نگهداری نمایید. شناسایی ریسک و تهدیدات امنیتی روشهای ارزیابی و کنترل باید به عنوان حداقل پیش نیاز) متناسب با ماهیت و مقیاس عملیات (سازمان) باشد. این ارزیابی باید احتمال وقوع یک واقعه و طبعات آن که شامل موارد زیر می باشد را در نظر گیرد:

الف) ریسک ها و تهدیدات خطای فیزیکی، از قبیل خطای عملیاتی خسارت تصادفی، خسارت با سوءِ نظر و یا عمل جنایی و تروریستی.

ب) ریسک ها و تهدیدات عملیاتی، شامل کنترل امنیت، فاکتورهای انسانی و دیگر فعالیتهایی که عملکرد، شرایط و ایمنی سازمان را تحت تأثیر قرار دهد.

ج) اتفاقات محیط زیستی (طوفان، سیل و غیره) که می تواند اقدامات امنیتی را مانع شده و تجهیزات را بی اثر نماید.

د) عوامل خارج از کنترل سازمان از قبیل خدمات و تجهیزات عرضه شده از خارج از سازمان.

ه) تهدیدات و ریسکهای (ناشی از) ذینفع از قبیل عدم رعایت الزامات قانونی یا خسارت به آبرو (آبروی سازمان) و برند (مارک تجاری) سازمان.

و طراحی و نصب تجهیزات امنیتی شامل جایگزینی و تعمیرات آنها و غیره؛

ز) اطلاعات (سازمان) و مدیریت داده ها و ارتباطات؛

ح) تهدیدی (از هر نوع) برای تداوم عملیات؛

سازمان باید اطمینان حاصل نماید که نتایج این ارزیابی ها و تاثیرات این کنترل ها مورد توجه قرار گرفته اند و هر جا مناسب باشد ورودی لازم برای موارد زیر را فراهم سازد.

الف) انتظارات (کلی) و اهداف (خرد) مدیریت امنیت؛

ب) برنامه های مدیریت امنیت؛

ج) تعیین نیازهای طراحی مشخصه ها و نصب (تجهیزات مرتبط با امنیت سازمان)؛

د) شناسایی منابع کافی از جمله سطح نیروهای انسانی لازم (تعداد پرسنل مورد نیاز)؛

ه) شناسایی نیازهای آموزشی و مهارت ها (به بند ٤-٤-٢ مراجعه شود)،

و) توسعه کنترل های عملیاتی به بند ٤-٤-۶ مراجعه شود)،

ز) چهارچوب کلی مدیریت تهدید و ریسک (متوجه) سازمان.

سازمان باید اطلاعات فوق را مستند سازی کرده و به روز رسانی نماید. منطق انتخاب روش مورد استفاده توسط سازمان برای شناسایی و ارزیابی ریسک باید:

الف) با در نظر گرفتن دامنه کاربرد ماهیت و برنامه زمانی این اطمینان را بدهد که (روش مورد استفاده) عاملانه است و نه عکس العملی.

ب) شامل جمع آوری اطلاعات مرتبط با تهدیدات و ریسک های امنیتی باشد.

ج) امکان طبقه بندی تهدیدات ریسکها و شناسایی آن دسته (از آنها) که باید از آنها پرهیز شود حذف شوند و یا کنترل شوند را فراهم سازد.

د) امکان پایش عملیات را فراهم سازد تا از مؤثر بودن و به موقع بودن از نظر زمانی و به کارگیری (مناسب) آنها اطمینان حاصل شود به بند ٤-٥-١ مراجعه شود).

٤-٣-٢- الزامات،قانونی دولتی و دیگر الزامات کنترلی امنیت

سازمان باید برای اقدامات زیر روشهای اجرایی تهیه، نگهداری و به کار گیرد.

الف) شناسایی و پیدا کردن دسترسی به الزامات قانونی مورد کاربرد به رعایت آنها در ارتباط با تهدید امنیتی و ریسک ها بوده و

ب) تعیین نحوه کاربرد این الزامات برای برطرف کردن تهدیدها و ریسک ها سازمان باید این امکانات را به روز رسانی نماید. (سازمان) باید اطلاعات مرتبط با الزامات قانونی و دیگر الزامات را به کارکنان اشخاص ثالث مرتبط از جمله پیمانکاران منتقل نماید.

٤-٣-٣- اهداف کلان مدیریت امنیت

سازمان باید اهداف کلان مدیریت امنیت را در فعالیت ها و سطوح مرتبط (در سازمان) به طور مستند تهیه کرده، نگهداری نموده و به اجرا گذارد. اهداف کلان باید منتج از و همخوان با خط مشی باشد.

در زمان تهیه و بازنگری اهداف کلان، سازمان باید موارد زیر را در نظر گیرد:

الف) الزامات قانونی دولتی و دیگر ضوابط کنترلی امنیت؛

ب تهدیدها و ریسک های مرتبط با امنیت؛

ج) گزینه های تکنولوژیکی و دیگر گزینه ها)؛

د) الزامات تجاری عملیاتی و مالی؛

ه) نظرات ذینفعان مرتبط

اهداف کلان مدیریت امنیت باید:

الف) همخوان با تعهد سازمان به بهبود مستمر باشد.

ب) قابلیت اندازه گیری داشته باشد (در صورت عملی بودن).

ج) به کلیه کارکنان مرتبط و شخص های ثالث از جمله پیمانکاران اطلاع رسانی شود و با این هدف که این افراد نسبت به وظایف (تعهدات) فردی خود آگاه شوند.

د) در فواصل زمانی مورد بازنگری قرار گیرد تا از مرتبط و همخوان بودن با خط مشی مدیریت امنیت اطمینان حاصل شود. هر جا لازم باشد، اهداف کلان مدیریت امنیت باید قابلیت تغییر بر حسب مورد را داشته باشد.

٤-۳-٤- اهداف خرد مدیریت امنیت

سازمان باید اهداف خرد مدیریت امنیت را به طور مناسب با نیازهای سازمان به طور مستند تهیه به اجرا گذاشته و نگهداری نماید.

اهداف خرد باید منتج از و همخوان با اهداف کلان مدیریت امنیت باشد.

این اهداف باید:

الف) به طور مناسب دارای جزئیات باشد؛

ب) مشخص، قابل اندازه گیری قابل دستیابی مرتبط و مبتنی بر زمانبندی. (در صورت کاربرد داشتن) باشند. (اهداف باید SMART باشند):

ج) به کلیه کارکنان مرتبط شخص های ثالث از جمله پیمانکاران اطلاع رسانی شود، با این نیت (قصد) که این افراد از وظایف (تعهدات) خود آگاه شوند؛

د) در فواصل زمانی مورد بازنگری قرار گیرد تا از مرتبط و همخوان بودن با اهداف کلان مدیریت امنیت اطمینان حاصل شود. اهداف چنانچه ضروری باشد باید بر حسب مورد تغییر داده شوند.

٤-۳-۵- برنامه های مدیریت امنیت

سازمان باید برنامه های مدیریت امنیت برای دستیابی به اهداف کلان و خرد را تهیه نموده، به اجرا گذاشته و نگهداری نماید.

برنامه ها باید تا حد امکان جامع و کاربردی بوده و سپس با رعایت حق تقدم به اجرا گذاشته شود و سازمان باید برای به اجرا گذاشتن مؤثر و مقرون به صرفه آنها اقدام نماید.

این برنامه ها باید مستندات مربوط به تشریح موارد زیر را در بر گیرد:

الف) تعیین مسئولیت و اختیارات برای دستیابی به اهداف کلان و خرد مدیریت امنیت؛

ب) امکانات و برنامه زمانبندی که طی آن اهداف کلان و خرد مدیریت امنیت باید محقق شوند.

برنامه های مدیریت امنیت باید در فواصل زمانی مورد بازنگری قرار گیرد تا از مؤثر بودن و همخوان بودن آنها با اهداف کلان و خرد (مدیریت امنیت) اطمینان حاصل شود. در صورت نیاز برنامه ها باید به طور مناسب با مورد تغییر داده شوند.

٤-٤- اجرا و عملیات

٤-٤-١- ساختار، اختیارات و مسئولیتها برای مدیریت امنیت

سازمان باید ساختار، وظایف، مسئولیتها و اختیارات را همخوان با دستاورد خط مشی مدیریت امنیت اهداف کلان، اهداف خرد و برنامه ها تهیه و نگهداری نماید.

این وظایف، مسئولیتها و اختیارات باید تعریف شده، مستند سازی شده و به افراد مسئول برای استقرار و نگهداری اطلاع رسانی شود.

مدیریت ارشد باید شواهدی دال بر تعهدات خود برای توسعه و به کارگیری سیستم مدیریت امنیت و بهینه سازی مستمر و مؤثر بودن آن را از طرق زیر تهیه نماید:

الف) فردی را از رده مدیریت ارشد منصوب نماید که جدا از دیگر مسئولیت ها، مسئول طراحی کلی، نگهداری مستندسازی و بهینه سازی سیستم مدیریت امنیت سازمان باشد.

ب) انتصاب فرد (افرادی) از تیم مدیریت با اختیارات لازم جهت اطمینان از اینکه اهداف کلان و خرد به اجرا گذاشته شده اند.

ج) شناسایی و پایش نیازها و توقعات ذینفعان سازمان و اتخاذ تصمیمات مناسب و به موقع جهت مدیریت این گونه توقعات؛

ه) اطمینان یافتن از دسترسی به منابع کافی؛

د) مورد توجه قرار دادن تاثیر نامطلوبی که خط مشی مدیریت امنیت، اهداف کلان، اهداف خرد و برنامه ها و غیره ممکن است بر جنبه های دیگر سازمان بگذارد.

و) اطمینان یافتن از این که هر برنامه امنیتی که در قسمت های دیگر سازمان تهیه شده مکمل سیستم مدیریت امنیت می باشد.

ز) اطلاع رسانی اهمیت رعایت الزامات مدیریت امنیت به کارکنان سازمان در راستای تحقق خط مشی سازمان؛

ح) اطمینان یافتن از این که تهدیدات و ریسک های مرتبط با امنیت مورد ارزیابی قرار گرفته و در سنجش های تهدید ریسک به گونه مناسب لحاظ می شوند.

ط) اطمینان یافتن از قابلیت تحقق پذیری اهداف کلان، اهداف خرد و برنامه های مدیریت امنیت.

٤-٤-٢- صلاحیت آموزش و آگاهی

سازمان باید اطمینان حاصل نماید که افراد مسئول طراحی، عملیات و مدیریت فرآیندها و تجهیزات

امنیتی از نظر آموزش و / یا تجربیات واجد صلاحیت می باشند. سازمان باید روش های اجرایی را به منظور آگاه کردن از موارد زیر تهیه و نگهداری نماید:

الف) اهمیت رعایت خط مشی مدیریت امنیت و روش های اجرایی و الزامات سیستم مدیریت امنیت؛

ب) وظایف و مسئولیت ها در راستای رعایت خط مشی مدیریت است. روشهای اجرایی و الزامات سیستم مدیریت امنیت شامل آمادگی در شرایط اضطراری و الزامات واکنش (به شرط اضطراری)

ج) طبعات بالقوه متصور برای امنیت سازمان در صورت عدول از روشهای اجرایی مشخص (برای روبرو شدن با هر وضعیت)

سوابق صلاحیت و آموزش باید نگهداری شود.

٤-٤-٣- ارتباطات

سازمان باید با استفاده از روشهای اجرایی اطلاعات مناسب و مقتضی در مورد مدیریت امنیت را به کارکنان مرتبط، پیمانکاران و دیگر ذینفعان اطلاع رسانی نماید. به دلیل ماهیت حساس برخی اطلاعات مربوط به امنیت توجه کافی باید معطوف حساسیت اطلاعات قبل از ارسال آنها گردد.

٤-٤-٤- مستندات

سازمان باید یک سیستم مستندات مدیریت امنیت را که شامل و نه محدود به موارد زیر می باشد، تهیه و نگهداری نماید.

الف) خط مشی (برای) امنیت اهداف کلان و خرد؛

ب) شرح دامنه کاربرد سیستم مدیریت امنیت؛

ج) شرح اجزاءِ اصلی سیستم مدیریت امنیت و تأثیر آنها بر یکدیگر و فهرست مستندات مرتبط

د) مستندات شامل سوابق مورد نیاز این استاندارد بین المللی و

ه) مستندات شامل سوابقی که از نظر سازمان ضروری تعیین شده به منظور اطمینان از طرح ریزی مؤثر عملیات و کنترل فرآیندهایی که مرتبط با تهدیدات و ریسکهای بارز آن (سازمان) می باشد.

سازمان باید حساسیت امنیتی اطلاعات خود را تعیین کرده و برای جلوگیری از دسترسی غیر مجاز (به آنها) قدم بردارد (اقدام نماید).

٤-٤-٥- کنترل داده ها و مستندات

سازمان باید روشهای اجرایی را برای کنترل مستندات، داده ها و اطلاعات طبق خواسته بند ٤ این استاندارد بین المللی تهیه و نگهداری نماید تا اطمینان یابد:

الف) این مستندات داده ها و اطلاعات قابلیت ردیابی داشته و تنها توسط افراد مجاز قابل دسترسی می باشند.

ب) این مستندات، داده ها و اطلاعات در فواصل زمانی مورد بازنگری و بازسازی در صورت نیاز قرار گرفته و از نظر کفایت توسط افراد مجاز مورد تأیید قرار می گیرند.

ج) ویرایش جاری به روز مستندات داده ها و اطلاعات در مکان هایی که عملیات اساسی از نظر عملکرد

مؤثر سیستم مدیریت امنیت انجام می شود در دسترس می باشند.

د) مستندات داده ها و اطلاعات منسوخ در اسرع وقت از کلیه مکان های نشر و استفاده جمع آوری شده و یا از عدم استفاده ناخواسته آنها اطمینان حاصل می شود.

ه) مستندات داده ها و اطلاعاتی که به دلایل قانونی و یا به جهت حفظ دانش یا هر دو در آرشیو نگهداری میشوند به طور مناسب قابل دسترسی می باشند.

و) این مستندات داده ها و اطلاعات در جای امن قرار گرفته و چنانچه به صورت الکترونیکی میباشند دارای (سیستم) پشتیبانی بوده و قابل بازیافت می باشند.

٤-٤-۶- کنترل عملیات

سازمان باید آن دسته از فعالیتها و عملیات را که برای دستیابی به موارد زیر ضروری می باشد شناسایی نماید:

الف) خط مشی مدیریت امنیت؛

ب) کنترل فعالیت ها و کاهش تهدیدات شناسایی شده که دارای ریسک بارز می باشند؛

ج) رعایت الزامات قانونی، دولتی و دیگر ضوابط امنیتی؛

د) اهداف کلان مدیریت امنیت (سازمان)؛

ه) به اجرا گذاشتن برنامه های مدیریت امنیت؛

و) سطح مورد نیاز برای امنیت زنجیره تأمین (منظور حد امنیت مورد نیاز)

سازمان باید از طرق زیر اطمینان حاصل نماید که این فعالیت ها و عملیات تحت شرایط مشخص شده انجام می گیرد:

الف) تهیه استقرار و نگهداری روشهای اجرایی مستند به منظور کنترل موقعیت هایی که نبود آنها روشهای اجرایی منجر به شکست در دستیابی به عملیات و فعالیتهایی که در بند ٤-٤-۶ الف تا و در فوق ذکر شده می گردد؛

ب) ارزیابی تهدیدهایی که از فعالیت های زنجیره تأمین بالا دست متوجه سازمان می شود و بکارگیری کنترلها به منظور کاهش این گونه اثرات به سازمان و دیگر فعالان در زنجیره تأمین پایین دست؛

ج) تهیه و نگهداری الزامات برای کالاها و خدماتی که بر امنیت تاثیر گذار بوده و منتقل کردن این (موارد) به تأمین کنندگان و پیمانکاران

این روشهای اجرایی باید کنترلهای طراحی نصبت عملیات دارسازی و تغییرات کاربردی اجزاء تجهیزات مرتبط با امنیت ابزار دقیق و غیره طور مناسب را شامل گردد.

هر جا که ترتیبات موجود مورد بازسازی قرار میگیرد و یا ترتیبات جدید معرفی می گردد که بتواند بر عملیات و فعالیتهای مدیریت امنیت تأثیر گذار باشد سازمان باید تهدیدها و ریسکهای مرتبط با امنیت آنها را قبل از بکارگیری آنها مورد توجه قرار دهد. ترتیبات جدید و یا بازنگری شده ای که در نظر گرفته میشوند باید موارد زیر را شامل شوند.

الف) ساختار وظایف و مسئولیت های بازنگری شده سازمان

ب) خط مشی بازنگری شده امنیت، اهداف کلان و اهداف خود و برنامه ها (برای دستیابی به اهداف)

ج) فرآیندها و روشهای اجرایی بازنگری شده

د) به کارگیری زیر ساخت های جدید، تجهیزات یا فن آوری امنیتی که می تواند شامل سخت افزار و نرم افزار باشد.

ه) معرفی پیمانکاران تأمین کنندگان و پرسنل جدید به گونه مناسب با وضعیت (پس از بازنگری)

٤-٤-٧- آمادگی در شرایط اضطراری واکنش و بازیافت امنیت

سازمان باید طرح ها و روشهای مناسب را برای شناسایی توان (سازمان) برای واکنش در مقابل موارد امنیتی و وضعیت های اضطراری و به منظور جلوگیری و کاهش عواقب منصور در ارتباط با آنها تهیه کرده، به اجرا گذاشته و نگهداری نماید.

این طرح ها و روش ها باید اطلاعات در مورد فراهم سازی و نگهداری هر دستگاه شناسایی شده اطلاعات یا خدماتی که می تواند در طی یا بعد از حوادث و یا موقعیتهای اضطراری مورد نیاز باشد را شامل گردد.

سازمان باید در فواصل، زمانی کارایی آمادگی خود را در شرایط اضطراری عکس العمل طرح های بازیابی امنیت و روشهای اجرایی به نا خصوص پس از وقوع حوادث یا وضعیتهای اضطراری ناشی از نقص های امنیتی و تهدیدها مورد بازنگری قرار دهد.

سازمان باید در فواصل زمانی این روشها را هر جا که امکان پذیر باشد مورد آزمایش قرار دهد (به عنوان مثال با برگزاری مانورهای امنیتی)

٤-٥- کنترل (رسیدگی و اقدام اصلاحی)

٤-٥-١- پایش و اندازه گیری عملکرد امنیتی

سازمان باید روش های اجرایی را به منظور پایش و اندازه گیری عملکرد سیستم مدیریت امنیت خود تهیه و نگهداری نماید.

(سازمان) همچنین باید روشهای اجرایی را برای پایش و اندازه گیری ۷ عملکرد امنیتی خود تهیه و نگهداری نماید. سازمان باید تهدیدها و ریسک های وابسته را شامل مکانیزم های بدتر شدن (تضعیف) توانایی (سازمان) و عواقب آن در زمانی که تواتر اندازه گیری و پایش پارامترهای کلیدی عملکرد خود را تعیین می کند، مورد توجه قرار دهد.

این روش ها باید موارد زیر را امکان پذیر سازد:

الف) هر دو اندازه گیریهای کیفی و کمی متناسب با نیازهای سازمان

ب) پایش میزان دستیابی سازمان به خط مشی اهداف کلان و اهداف خرد مدیریت امنیت؛

ج) انتخاب شاخصهای عاملانه عملکرد که رعایت برنامه های مدیریت امنیت معیارهای کنترل عملیات و قوانین مرتبط دولتی و دیگر الزامات ضوابطی را مورد پایش قرار می دهند؛

د) شاخص های عکس العملی عملکرد به منظور پایش زوال از دست رفتن جایگاه و توانایی مرتبط با امنیت

عدم موفقیت ها، حوادث، عدم انطباق ها (شامل شبه حوادث هشدارهای خلاف واقع) و دیگر شواهد ثبت شده در گذشته مربوط به ضعف در عملکرد سیستم مدیریت امنیت

ه) ثبت داده ها و نتایج پایش و اندازه گیری ها به حد کافی برای تجزیه و تحلیل (اثر بخشی) اقدامات اصلاحی و بازدارنده بعدی که سازمان پس از موارد ذکر شده در بند د باید انجام دهد).

اگر نیاز به تجهیزات پایش برای عملکرد و یا اندازه گیری و پایش باشد. سازمان ملزم است تا روش های اجرایی برای کالیبراسیون و نگهداری این گونه تجهیزات را تهیه و نگهداری نماید.

سوابق کالیبراسیون و فعالیتهای نگهداری (تعمیرات) و نتایج حاصله باید. برای مدت کافی با رعایت قوانین دولتی موجود و خط مشی سازمان نگهداری شود.

٤-٥-٢- ارزیابی سیستم

سازمان باید طرحهای مدیریت امنیت روش ها و توانایی هایش را از طریق بازنگری های ادواری آزمون گزارش های تهیه شده پس از وقوع حوادث درسهای آموخته شده ارزیابی عملکرد و تجربیات را مورد ارزیابی قرار دهد. تغییرات بارز (عمده) در این عوامل باید بدون فوت وقت در روش روشهای اجرایی منعکس گردد.

سازمان باید به طور ادواری میزان رعایت ضوابط قانونی و مقررات روش های بهینه مورد استفاده در صنعت مرتبط با فعالیت اش و انطباق با خط مشی و انتظارات خود را از سیستم مدیریت امنیت) ارزیابی نماید. سازمان باید سوابق نتایج ارزیابیهای ادواری را نگهداری نماید.

٤-٥-٣- عدم موفقیتهای مرتبط با امنیت وقایع، عدم تطابقها و اقدام اصلاحی و پیشگیرانه

سازمان باید روشهای اجرایی را تهیه کرده به اجرا گذاشته و نگهداری نماید تا مسئولیت و اختیارات را برای فعالیتهای زیر تعریف نماید:

الف) ارزیابی و به اجرا گذاری اقدامات پیشگیرانه به منظور شناسایی عدم موفقیت های بالقوه در امور مربوط به امنیت با این هدف که از وقوع آنها در آینده جلوگیری نماید؛

ب) تحقیقات در مورد موارد مرتبط با امنیت شامل؛

۱) عدم موفقیت ها از جمله شبه حوادث و هشدارهای خلاف واقع؛

۲) وقایع و وضعیت های اضطراری؛

۳) عدم انطباق ها؛

ج) اقدام جهت کاهش اثرات هر گونه عواقب ناشی از عدم موفقیت ها، وقایع یا عدم انطباق ها؛

د) به اجرا گذاشتن و تکمیل اقدامات اصلاحی؛

ه) تایید موثر بودن اقدامات اصلاحی انجام شده (این که اقدامات اصلاحی موثر بوده اند)

چنین روش های اجرایی لازم می دارد که کلیه اقدامات اصلاحی و پیشگیرانه از طریق فرایند سنجش ریسک و تهدید امنیتی، قبل از به اجرا گذاشتن، مورد بازنگری قرار گیرد مگر آنکه بکارگیری فوری آنها مانع از به خطر افتادن جان و ایمنی مردم گردد (یعنی که در اینصورت باید فورا و قبل از بازنگری به اجرا گذاشته

شوند)

هرگونه اقدام اصلاحی یا پیشگیرانه به منظور حذف علل عدم انطباق های واقعی یا بالقوه باید متناسب با اندازه (بزرگی- کوچکی) مشکلات بوده و همخوان با تهدیدها و ریسک های احتمالی که مدیریت امنیت با آنها مواجه خواهد شد باشد. سازمان باید هر نوع تغییرات در روش های اجرایی مستند ناشی از اقدام اصلاحی و پیشگیرانه انجام شده را ثبت نماید و هر جا ضروری باشد نیاز به آموزش را (به دلیل تغییرات ایجاد شده) مورد نظر قرار دهد.

٤-٥-٤- کنترل سوابق

سازمان باید سوابق مورد نیاز برای نشان دادن انطباق با الزامات سیستم مدیریت امنیت خود و این استاندارد و نتایج به دست آمده را تهیه و نگهداری نماید.

سازمان باید روش (روش های) اجرایی را برای شناسایی، ذخیره، محافظت، بازیابی، جمع آوری و منسوخ نمودن سوابق تهیه نموده به اجرا گذاشته و نگهداری نماید.

سوابق باید خوانا، قابل شناسایی و قابل ردیابی بوده و (به همین صورت) باقی نماند.

مستندات الکترونیکی و دیجیتال باید مصون از دستکاری بوده، دارای پشتوانه ایمن بوده و فقط توسط افراد مجاز قابل دسترسی باشد.

٤-٥-٥- ممیزی

سازمان باید برنامه ممیزی مدیریت امنیت را تهیه کرده به اجرا گذاشته و نگهداری نماید و باید اطمینان یابد که ممیزی های سیستم مدیریت امنیت در فواصل زمانی برنامه ریزی شده صورت می گیرد به این منظور که:

الف) تعیین نماید که سیستم مدیریت امنیت موارد زیر را نشان می دهد یا نمی دهد. (انطباق یا عدم انطباق را نشان دهد)

۱- با ترتیبات طرح ریزی شده برای مدیریت امنیت شامل الزامات مندرج در کل بند ٤ این مشخصه، انطباق دارد.

۲- بطور صحیح استقرار یافته و نگهداری شده است.

۳- در تحقیق یافتن خط مشی و انتظارات (از سیستم مدیریت امنیت) موثر بوده است.

ب) بازنگری نتایج ممیزی های قبلی و اقدامات انجام شده در مورد رفع عدم انطباق ها.

ج) تهیه اطلاعات در مورد نتایج ممیزی برای مدیریت.

د) صحه گذاری بر اینکه تجهیزات امنیتی و پرسنل (مرتبط با مسائل امنیت) بطور مطلوب (موثر) به کار گرفته شده اند.

برنامه ممیزی شامل هر گونه زمانبندی باید بر مبنای نتایج سنجش تهدید و ریسک فعالیت های سازمان و نتایج ممیزی های قبل تدوین گردد.

روش های انجام ممیزی باید دامنه کاربرد، تواتر زمانی، استفاده از متدها (منظور متدهای انجام ممیزی)

شایستگی (منظور شایستگی افرادی که ممیزی را انجام می دهند) و نیز مسئولیت ها و الزامات انجام ممیزی و گزارش دهی نتایج را پوشش دهد. هر کجا که امکان پذیر باشد، ممیزی ها توسط افراد مستقل (وجدا) از آنهایی که مسئولیت مستقیم برای فعالیت مورد آزمون (منظور ممیزی) را دارند صورت گیرد.

یادآوری: جمله افراد مستقل الزاما به معنی افراد خارج از سازمان نمی باشد.

٤-۶- بازنگری مدیریت و بهبود مستمر

مدیریت ارشد باید سیستم مدیریت امنیت سازمان را در فواصل زمانی برنامه ریزی شده مورد بازنگری قرار دهد تا از تداوم مناسب بودن (قابل قبول بودن) کفایت (در جهت پوشش دادن کلیه فعالیت های سازمان) و موثر بودن آن (در جلوگیری از وقوع حوادث امنیتی) اطمینان حاصل نماید. بازنگری ها باید شامل سنجش موفقیت ها برای بهبود و نیاز به تغییرات در سیستم مدیریت امنیت بوده، خط مشی امنیتی و انتظارات و تهدیدها و ریسک های امنیتی را نیز دربرگیرد. (اطلاعات) و وردی برای بازنگری های مدیریت شامل موارد زیر می باشد:

الف) نتایج ممیزی ها و ارزیابی های میزان رعایت الزامات قانونی و دیگر الزاماتی که سازمان باید آنها را رعایت نماید.

ب) تماس (تماس ها) از طرف گروه های علاقمند (به سازمان) از خارج از سازمان، از جمله شکایات.

ج) عملکرد امنیتی سازمان؛

د) میزان دستیابی به انتظارات و اهداف (امنیتی)

ه) وضعیت اقدامات اصلاحی و پیشگیرانه؛

و) اقدامات پیگیرانه از بازنگری های قبلی مدیریت؛

ز) مقتضیات تغییر یافته شامل تغییرات در الزامات قانونی و دیگر الزامات در ارتباط با جنبه های امنیتی و

ح) پیشنهادات برای بهبود.

خروجی های بازنگری های مدیریت باید شامل تصمیمات و اقدامات مرتبط با تغییرات ممکن در خط مشی امنیتی، انتظارات (از سیستم مدیریت امنیت) ، اهداف و دیگر اجزای سیستم مدیریت امنیت در همخوانی با تعهد برای بهبود مستمر باشد.